Fall 2014

# Beyond the Schoolhouse Gates: The Unprecedented Expansion of School Surveillance Authority Under Cyberbullying Laws

Emily F. Suski
*Georgia State University College of Law*, esuski@gsu.edu

# Beyond the Schoolhouse Gates: The Unprecedented Expansion of School Surveillance Authority Under Cyberbullying Laws

*Emily F. Suski*[†]

Abstract

For several years, states have grappled with the problem of cyberbullying and its sometimes devastating effects. Because cyberbullying often occurs between students, most states have understandably looked to schools to help address the problem. To that end, schools in forty-six states have the authority to intervene when students engage in cyberbullying. This solution seems all to the good unless a close examination of the cyberbullying laws and their implications is made. This Article explores some of the problematic implications of the cyberbullying laws. More specifically, it focuses on how the cyberbullying laws allow schools unprecedented surveillance authority over students. This authority stands in notably stark contrast to the constraints on government authority in other contexts, including police authority to search cell phones. In June 2014, the Supreme Court recognized in *Riley v. California* that police searches of cell phones require a warrant because of the particular intrusions into privacy attendant to those searches. While some surveillance authority over students may be warranted, the majority of the cyberbullying laws implicitly give schools unlimited, or nearly unlimited, and unfettered surveillance authority over students' online and electronic activity whenever, wherever, and however it occurs: at home, in bedrooms, at the mall, on personal cell phones, on tablets, or on laptops.

† Assistant Clinical Professor, Georgia State University College of Law. LL.M., Georgetown University Law Center; J.D., University of North Carolina. I am grateful to the following individuals for the very helpful feedback they provided on this Article: Scott Bauries, Marion Crain, Lauren Sudeall Lucas, Jessica Steinberg, Jonathan Todres, and Mark Weber. I am also grateful to the participants of the University of Kentucky College of Law Developing Ideas Conference and the Association of American Law Schools Conference on Clinical Legal Education Works in Progress session for feedback on earlier versions of this Article. Finally, I owe thanks to John Sharpe for outstanding research assistance.

This Article argues that the cyberbullying laws, though well meaning, vastly expand school authority through the broad, if implicit, allowance of surveillance authority over students and implicate privacy harms that are made more acute because the authority lies with schools over students. Although no doctrine yet exists on the limits of school surveillance authority, limits on school authority in other contexts do exist. First and Fourth Amendment doctrine in student-speech and search cases, as well as doctrine on government surveillance more generally, offers some guidance on where the boundaries of school authority lie. The surveillance authority in most cyberbullying laws goes beyond these bounds, indicating that cyberbullying laws expand school authority. To protect students from excessive school surveillance authority and attendant privacy harms, realistic limits need to be imposed on school surveillance authority under the cyberbullying laws both by way of a framework for determining the boundaries of school authority and a cause of action for students. This Article calls for both and draws on the nexus doctrine in First Amendment student-speech cases to develop such a framework.

## CONTENTS

## INTRODUCTION

Although much attention has deservedly been paid to the problem of cyberbullying, little attention has been paid to some of the far-reaching implications of the anti-cyberbullying laws that collectively represent the response to the problem. This Article explores some of the unexamined and troubling aspects of the cyberbullying laws. Cyberbullying laws, mostly passed as part of states' education codes, prohibit cyberbullying, or bullying by electronic means, and provide schools with the authority to discipline students for it.[1] California

1. ALA. CODE § 16-28B (2012); ARIZ. REV. STAT. ANN. § 15-341 (2012); ARK. CODE ANN. § 6-18-514 (2009); CAL. EDUC. CODE § 48900(r) (West Supp. 2014); COLO. REV. STAT. § 22-32-109.1 (2012); CONN. GEN. STAT. ANN. § 10-222d (Supp. 2014); DEL. CODE ANN. tit. 14, § 4112D (Supp. 2012); FLA. STAT. ANN. § 1006.147 (West Supp. 2014); GA. CODE ANN. § 20-2-751.4 (2012); HAW. CODE R. § 8-19-2 (LexisNexis 2014); 105 ILL. COMP. STAT. ANN. 5/27-23.7 (West 2012); IND. CODE ANN. § 20-33-8-0.2 (West Supp. 2014); IOWA CODE § 280.28. (2011); KAN. STAT. ANN. § 72-8256 (Supp. 2013); LA. REV. STAT. ANN. § 17:416.13 (Supp. 2014); LA. REV. STAT. ANN. § 14:40.7 (Supp. 2014); ME. REV. STAT. tit. 20-A, § 6554 (Supp. 2013); MD. CODE ANN., EDUC. § 7-424 (LexisNexis 2012); MASS. GEN. LAWS ANN. ch. 71, § 37O (West Supp. 2014); MICH. COMP. LAWS ANN.§ 380.1310b (West 2013); MINN. STAT. ANN. § 121A.0695 (West 2008); MISS. CODE ANN. § 37-11-67 (Supp. 2013); MO. REV. STAT. § 160.775 (2010); NEB. REV. STAT. § 79-2,137 (Supp. 2013); NEV. REV. STAT. §§ 388.135, 388.1351 (Supp. 2013); N.H. REV. STAT. ANN. § 193-F (2011); N.J. STAT. ANN. § 18A:37-14 (West 2013); N.M. CODE R. § 6.12.7.7 (LexisNexis 2014); N.Y. EDUC. LAW §§ 11–12 (McKinney Supp. 2014); N.C. GEN. STAT. § 115C-407.15 (2011); N.D. CENT. CODE § 15.1-19-17 to -18 (Supp. 2013); OHIO REV. CODE ANN. § 3313.666 (LexisNexis 2013); OKLA. STAT. tit. 70, §§ 24-100.2 to 24-100.5 (Supp. 2013); OR.

enacted one of the first such laws in 2008,[2] and forty-six states and the District of Columbia now have laws prohibiting cyberbullying.[3]

The laws are a response to both the increased attention to the problem of cyberbullying over the last several years and calls-to-action to address it.[4] These calls have been made for good reason; cyberbullying is a prevalent, sometimes tragic, problem.[5] According to

---

REV. STAT. §§ 339.351, 339.356 (2011); 24 PA. CONS. STAT. ANN. § 13-1303.1-A (West Supp. 2014); R.I. GEN. LAWS §§ 16-21-33 to 16-21-34 (Supp. 2013); S.C. CODE ANN. §§ 59-63-120 to 59-63-150 (Supp. 2013); S.D. CODIFIED LAWS §§ 13-32-14 to 13-32-14 (Supp. 2013); TENN. CODE ANN. §§ 49-6-4502 to 49-6-4503 (2013); TEX. EDUC. CODE ANN. § 37.0832 (West 2014); UTAH CODE ANN. § 53A-11a (LexisNexis Supp. 2013); VT. STAT. ANN. tit. 16, §§ 11, 570 (Supp. 2013); VA. CODE ANN. §§ 22.1-276.01, 22.1-291.4 (Supp. 2014); WASH. REV. CODE § 28A.300.285 (2012); W. VA. CODE ANN. § 18-2C (LexisNexis 2012); WYO. STAT. ANN. §§ 21-4-312 to 21-4-312 (2011). The District of Columbia also has a law prohibiting bullying, but it is not contained in its education code. Instead it is part of its government affairs statutes. Nonetheless, the statute requires schools to adopt the definition of bullying, including cyberbullying. D.C. CODE §§ 2-1535.01 to 2-1535.09. As another example, Idaho's bullying statute is part of its penal code, though it only refers to "student" actions. IDAHO CODE ANN. § 18-917A (2006).

2. Jeremy Thomas & Katy Murphy, *Cyberbullying: Parents, School Officials Both Search for Answers*, SAN JOSE MERCURY NEWS, May 2, 2013, http://www.mercurynews.com/ci_23158922/cyberbullying-parents-school-officials-both-search-answers.

3. Alaska, Kentucky, and Wisconsin do not include bullying by electronic means or any other definition of cyberbullying in their bullying laws. ALASKA STAT. § 14.33.200 (2012); KY. REV. STAT. ANN. § 525.070 (West 2006); WIS. STAT. ANN. § 118.46 (West Supp. 2013). Montana does not have a bullying law of any sort.

4. Scholars, journalists, and nonprofit groups, among others, have all called for action to address the problem. *E.g.*, Naomi H. Goodno, *How Public Schools Can Constitutionally Halt Cyberbullying: A Model Cyberbullying Policy That Considers First Amendment, Due Process, and Fourth Amendment Challenges*, 46 WAKE FOREST L. REV. 641 (2011) (advocating for a policy likely to survive a constitutional challenge); Kelly A. Albin, *Bullies in a Wired World: The Impact of Cyberspace Victimization on Adolescent Mental Health and the Need for Cyberbullying Legislation in Ohio*, 25 J.L. & HEALTH 155 (2012) (describing harms caused by cyberbullying and proposes legislation to address it); *Our Mission*, STOMP OUT BULLYING, http://www.stompoutbullying.org/index.php/about/mission/ (last visited June 24, 2014); (explaining mission to prevent bullying and cyberbullying, which sometimes leads victims to commit suicide) PACER CENTER'S NATIONAL BULLYING PREVENTION CENTER, http://www.pacer.org/bullying/nbpm/ (last visited June 24, 2014) (suggesting ways in which students, parents, and educators can take steps to raise bullying awareness).

5. *See generally* Lizette Alvarez, *Girl's Suicide Points to Rise in Apps Used by Cyberbullies*, N.Y. TIMES, Sept. 14, 2013 (describing how a

one study of twelve-to-seventeen-year-olds, 72 percent of Internet users reported at least one instance of bullying in the immediate prior year.[6] Of those in the study, 51 percent reported experiencing online bullying by other students in their school.[7] Given that this study was conducted in 2008, it seems reasonable to assume that the cyberbullying problem has not decreased with the increasing ubiquity of technology in the last few years, including new apps for texting and otherwise engaging through social media, some of which even provide for anonymous posting.[8]

Cyberbullying is not only a widespread problem but also one that can also have devastating effects. Rebecca Ann Sedwick serves as just one of many tragic examples of the effects of cyberbullying.[9] Rebecca was a twelve-year-old Florida girl who committed suicide in September 2013 by jumping off a platform at an abandoned cement plant after enduring more than a year of bullying by text message and over the Internet.[10]

By prohibiting cyberbullying among students, the cyberbullying laws are undoubtedly aimed at preventing more cases like Rebecca's and curbing the incidences of cyberbullying more generally. In intent, then, the laws heed the calls-to-action that have served as the catalyst for their enactment. Yet the manner in which the laws address the problem of cyberbullying creates its own set of problems. In a majority of states, they arguably provide schools with unlimited or nearly unlimited authority to conduct electronic surveillance of students' online and electronic activity whenever and wherever that activity occurs.

How do the cyberbullying laws provide schools with surveillance authority? By allowing schools the authority to discipline students for cyberbullying, they implicitly provide schools with the authority to ferret out the problem.[11] To determine whether and when students are engaged in cyberbullying, the schools have a few options, but among

---

twelve-year-old Florida girl committed suicide after being bullied on various texting and photo-sharing apps).

6. Jaana Juvonen & Elisheva F. Gross, *Extending the School Grounds? Bullying Experiences in Cyberspace*, 78 J. SCH. HEALTH 496, 502 (2009). The definitions of bullying in most bullying laws—twenty-eight—prohibit bullying that occurs as one-time acts. *See infra* note 26 and accompanying text.

7. *Id.* at 501–02.

8. Michael H. King, *Could the App Yik Yak Be a Cyberbullying Tool?* (Feb. 22, 2014, 12:33 AM), http://roswell.11alive.com/news/education/608482-could-app-yik-yak-be-cyberbullying-tool.

9. Alvarez, *supra* note 5, at A1.

10. *Id.*

11. *See infra* Part I.A.

the most effective and efficient means is developing a system for comprehensively monitoring students' online and electronic activity.[12] Because cyberbullying laws do not prohibit this surveillance, they arguably allow schools to reach into students' lives while they are at home, work, the mall or other non-school places and gather electronic data on the students in the name of learning about cyberbullying activity. The laws expand the proverbial schoolhouse gates to such a degree that, in many cases, schools' authority to conduct surveillance of students is nearly without bounds.[13]

Some schools are beginning to grab this implicit power under the cyberbullying laws to conduct just this level of surveillance. While the exercise of this implicit authority is new, at least a few schools and school districts have now hired (at no small expense) companies to comprehensively monitor the online and electronic activity of all their students at all locations and times. For example, in July 2014, Jackson County School District in North Carolina announced that it is paying a private company, Social Sentinel, $9,500 for one year to monitor the social media postings of all students in one of its high schools in order to uncover cyberbullying and other threats.[14] The school district's position is that when it comes to those kinds of threats, students have "'no expectation of privacy. That is the policy.'"[15] This surveillance—in Jackson County, North Carolina, and other schools that have started using similar services—occurs no matter whether the students are engaged in or are suspected of being engaged in cyberbullying activity or even whether the students are involved in any activity that has any relationship at all to the school or its pedagogical interests.[16] Potential abuses abound and actual

12. *Id.* School administrators have lamented the difficulty with catching online bullying. In the case of another student suicide attempt in California after other students taunted the student online and called her "ugly" and "a whore," the school principal investigated. However, she is quoted as saying, "'It was pretty awful for a while, and we couldn't substantiate any of it. It's like chasing a tail or a piece of yarn . . . .'" Thomas & Murphy, *supra* note 2.

13. In *Tinker v. Des Moines Indep. Sch. Dist.*, the Supreme Court found that students do not "shed their constitutional rights . . . at the schoolhouse gate." 393 U.S. 503, 506 (1969). Where those schoolhouse gates begin and end is now the question under cyberbullying laws. Part II will discuss the unprecedented breadth of surveillance authority currently provided to schools under these statutes.

14. Quintin Ellison, *School Officials to Monitor Students' Social Media Use*, SYLVIA HERALD, July 24, 2014, at 1A.

15. *Id.* (quoting Jackson Schools' Technology Director David Proffitt).

16. Somini Sengupta, *Warily, Schools Watch Students on the Internet*, N.Y. TIMES, Oct. 29, 2013, at A1; Kelly Wallace, *At Some Schools, "Big Brother" Is Watching* (Mar. 28, 2014, 9:31 PM), http://www.cnn.com/2013/11/08/living/schools-of-thought-social-media-monitoring-students/.

abuses have occurred. In 2010, school officials in Pennsylvania viewed students in their bedrooms because of surveillance made possible by the web cameras on school-issued laptops.[17] Yet because schools are under pressure to avoid blame for tragedies like student suicide, there is good reason to think that more will use the implicit surveillance authority under cyberbullying.[18]

It is with this surveillance authority that this Article is concerned. This Article argues that the cyberbullying laws, though well meaning, allow for an unprecedented expansion of school authority that implicates privacy harms, which are made more acute because the authority is held over the students by the schools. This grant of surveillance power to schools and its implications have largely gone overlooked by both scholars writing on the topic of bullying laws and privacy and surveillance studies scholars.[19] Drawing on the more general work of these scholars and locating cyberbullying laws in that literature, this Article examines this grant of authority to schools and its harms and then calls for changes in the laws both to limit school surveillance authority and the privacy harms created by that authority. It should be noted that the surveillance with which this Article is concerned is distinct from the disciplinary authority of the schools under the cyberbullying laws. The surveillance happens before any act occurs for which some discipline might be warranted. Whether that discipline is appropriate is a topic beyond the scope of this Article.

---

17. Suzan Clarke, *Pa. School Faces FBI Probe, Lawsuit, for Using Webcams on Laptops to Watch Students at Home* (Feb. 22, 2010), http://abcnews.go.com/GMA/Parenting/pennsylvania-school-fbi-probe-webcam-students-spying/story?id=9905488.

18. Indeed, even the companies that sell surveillance products and services to schools expect significant market growth. Wallace, *supra* note 16.

19. The bullying scholarship tends to cover the constitutional implications of bullying laws and whether they violate the First and Fourth Amendments. To this Author's knowledge, none of the scholarship addresses the surveillance authority implicit under cyberbullying laws or its privacy implications. *E.g.*, Goodno, *supra* note 4. (suggesting a regulatory framework for cyberbullying but not addressing the implicit authority currently available to states). There is no doctrine yet on what, if any, legal limits exist on school authority to conduct surveillance or its implications. However, privacy scholars have written about topics such as privacy rights and the harms implicated by broad-based government (as well as private) surveillance. *E.g.*, Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013); Danielle K. Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262 (2013); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006). Those privacy harms apply in the school surveillance context as well and provide theoretical and policy bases for the argument that school surveillance authority should have legal limits.

Part I of this Article catalogs the cyberbullying laws, explaining the three levels into which the grants of surveillance authority to schools fall: (1) the grant of authority requiring a substantial nexus to the school or school-related activities; (2) the grant of authority with a more limited nexus to the school or school-related activities; and (3) the grant of authority with no nexus to school or school-related activities. This Part also describes how broad the potential scope of the surveillance authority given to schools in the majority of states really is. To show that the broad surveillance authority represents an unprecedented expansion of school authority, Part II begins by discussing extant limits on the school authority under First and Fourth Amendment student-speech and search doctrine as well as doctrine on government surveillance more generally. Although there are no clear doctrinal limits on general, broad-based surveillance of students, this First and Fourth Amendment doctrine offers guidance on the limits of school authority more generally. So too does doctrine on government surveillance outside the school context; thus it also offers some guideposts for the limits on state and therefore school surveillance authority. This Part also explains how the surveillance authority under the majority of cyberbullying statutes exceeds or nearly exceeds all of these limits. While this expansion of school authority beyond its current limits might be deemed acceptable in the name of combatting cyberbullying, Part III explains why it is not: surveillance of students implicates privacy harms. This Part both outlines the privacy harms attendant to the enormous surveillance authority schools now have under the cyberbullying laws and contends that these harms are made more severe because the surveillance authority lies with the schools. Part IV then calls for changes in the cyberbullying laws both to limit schools' surveillance authority and the attendant privacy harms and to allow students to seek redress when those limits on school surveillance authority have been transgressed. This Part argues in favor of an analytical framework that uses the nexus theory of school authority, developed under the First Amendment line of student-speech cases, for defining school authority to conduct electronic surveillance of students.

## I. THE CYBERBULLYING LAWS AND THEIR THREE LEVELS OF SCHOOL SURVEILLANCE AUTHORITY

Under cyberbullying laws in the forty-six states and the District of Columbia, the grant of surveillance authority to schools falls into one of three categorical levels: (1) a grant of authority with no nexus to school or school-related activity;[20] (2) a grant of authority with a

20. See *infra* note 64 and accompanying text.

limited nexus to school or school-related activity;[21] and (3) a grant requiring a relatively substantial nexus to school or school-related activity.[22] The vast majority of cyberbullying laws provide schools with surveillance authority that falls into one of the first two categories. In those states, the schools have nearly unlimited or unlimited surveillance authority over students' online and electronic activity. Because it is perhaps easiest to understand the broadest grant of surveillance authority under cyberbullying laws by first understanding the most limited grant of authority under these laws, Part B of this section will first describe the most limited grant of school surveillance authority and work its way up through the other two categorical levels of school surveillance authority in ascending order. First, however, a more thorough description of the cyberbullying laws is warranted.

### *A. The Cyberbullying Laws' Implicit Authorization of Surveillance Authority*

While they vary in the details, bullying laws in general have some of the same basic elements, regardless of whether they have a cyberbullying component. Bullying laws are, for the most part, creatures of states' student disciplinary codes or regulatory schemes.[23] They either prohibit a student in a school from acting, even once, in a way that puts another student in reasonable fear of harm, or they prohibit a student in a school from engaging in potentially less severe but repeated behavior that effectively rises to the level of harassment.[24] Ten states prohibit only repeated acts of bullying.[25] Thirty-five states prohibit both one-time and repeated acts of bullying.[26] Nevada, for example, prohibits both a "willful act" or a

21. See *infra* note 64 and accompanying text.

22. See *infra* note 55 and accompanying text.

23. *See generally supra* note 22 and accompanying text.

24. *See generally supra* note 1 and accompanying text.

25. ALA. CODE § 16-28B (2012); CONN. GEN. STAT. ANN. § 10-222d(1) (Supp 2014); FLA. STAT. ANN. § 1006.147(3)(a) (Supp. 2014); IND. CODE ANN. § 20-33-8-0.2(a) (West Supp. 2014); MASS. GEN. LAWS ch. 71, § 37O(a) (West Supp. 2014); LA. REV. STAT. ANN. § 17:416.13(c) (Supp. 2014); N.M. CODE R. § 6.12.7.7(A) (LexisNexis 2014); OHIO REV. CODE ANN. § 3313.666(A) (LexisNexis 2013); S.D. CODIFIED LAWS § 13-32-15 (Supp. 2013); VT. STAT. ANN. tit. 16, § 11 (Supp. 2013).

26. ALASKA STAT. § 14.33.250(3) (2012); ARK. CODE ANN. § 6-18-514(b)(2) (2009); CAL. EDUC. CODE § 48900(r)(1) (West Supp. 2014); COLO. REV. STAT. § 22-32-109.1(b) (2012); DEL. CODE ANN. tit. 14, § 4112D(a) (Supp. 2012); GA. CODE. ANN. § 20-2-751.4(a) (West 2012); HAW. CODE R. § 8-19-2 (LexisNexis 2014); IDAHO CODE ANN. § 18-917A(2) (2006); IND. CODE § 20-33-8-02(a) 2007; KAN. STAT. ANN.

"course of conduct" if the act or course of conduct "places the person in reasonable fear of harm or serious emotional distress; or . . . creates an environment which is hostile to a pupil by interfering with the education of the pupil."[27]

Bullying laws proscribing a one-time act, behavior, or conduct stipulate that the act, behavior, or conduct be directed toward another student and put that student in reasonable fear of physical or emotional harm or result in similarly harmful effects.[28] Tennessee, for example, provides one definition of bullying as "any act that substantially interferes with a student's educational benefits, opportunities or performance; and . . . has the effect of [k]nowingly placing a student or students in reasonable fear of physical harm."[29]

For statutes effectively proscribing harassment, behavior is subject to discipline if it substantially interferes with the target student's educational performance or ability to benefit from the services or activities of school,[30] or substantially disrupts the orderly operations of the school.[31] In Iowa, "bullying" and "harassment" have the same definition in the school context.[32] They are defined as

§ 72-8256(a)(1)(A) (Supp. 2013); KY. REV. STAT. ANN. § 525.070 (West 2006); ME. REV. STAT. tit. 20-A, § 6554g(2)(c) (Supp. 2013); MD. CODE ANN., EDUC. § 7-424(a)(2) (West 2012); MICH. COMP. LAWS ANN. § 380.1310b(8)(b) (West 2013); MINN. STAT. ANN. § 121A.031(e) (West 2008); MISS. CODE ANN. § 37-11-67(1) (Supp. 2013); MO. ANN. STAT. § 160.775(2) (West 2010); NEV. REV. STAT. § 388.122 (Supp. 2013); N.H. REV. STAT. ANN. § 193-F:3 (2011); N.J. STAT. ANN. § 18A:37-14 (West 2013); N.Y. EDUC. LAW § 11(7) (McKinney Supp. 2014); N.C. GEN. STAT. § 115C-407.15(a) (2011); N.D. CENT. CODE § 15.1-19-17 (Supp. 2013); OKLA. STAT. tit. 70, § 24-100.3(c)(1) (Supp. 2013); OR. REV. STAT. § 339.351(2) (2011); 24 PA. CONS. STAT. ANN. § 13-1303.1-A(e) (West Supp. 2014); R.I. GEN. LAWS § 16-21-33(a)(1) (Supp. 2013); S.C. CODE ANN. § 59-63-120 (Supp. 2013); TENN. CODE ANN. § 49-6-4502(a) (2013); TEX. EDUC. CODE ANN. § 37.0832(a) (West Supp. 2014); UTAH CODE ANN. § 53A-11a-102 (LexisNexis Supp. 2013); VA. CODE ANN. § 22.1-276.01(A) (Supp. 2014); WASH. REV. CODE § 28A.300.285(2) (2012); W. VA. CODE ANN. § 18-2C-2(a) (LexisNexis 2012); WYO. STAT. ANN. § 21-4-312(a) (2011).

27. NEV. REV. STAT. § 388.122 (Supp. 2013).

28. *E.g.*, 105 ILL. COMP. STAT. ANN. 5/27-23.7(3) (West 2012).

29. TENN. CODE ANN. § 49-6-4502(a)(3) (2013).

30. *E.g.*, 105 ILL. COMP. STAT. ANN. 5/27-23.7(b)(3) (West 2012) (prohibiting bullying that, among other things, "substantially [interferes] with the student's or students' academic performance").

31. *E.g.*, MICH. COMP. LAWS ANN. § 380.1310b(8)(b)(iv) (West 2013) (prohibiting bullying that causes, among other things, a "substantial disruption in, or substantial interference with, the orderly operation of the school").

32. IOWA CODE § 280.28(2)(b) (2011).

conduct that "creates an objectively hostile school environment" and, among other things, "has the effect of substantially interfering with the student's ability to participate in or benefit from the services, activities, or privileges provided by a school."[33] In New Hampshire, the bullying statute prohibits bullying, which is defined as including "a pattern of incidents" that "substantially disrupts the orderly operation of the school."[34]

In most (twenty-five) states, cyberbullying laws are simply additions to or variations of these general definitions of bullying.[35] In these states, the relevant language typically specifies that bullying can happen by "electronic," among other, means.[36] Sixteen states, however, have separate statutory or regulatory definitions of cyberbullying.[37] These definitions are very similar to the general

33. IOWA CODE § 280.28(2)(b) (2011). In Iowa, as in other states with this harassment-like component to the cyberbullying statutes, the impact at school is not clearly subjective or objective. Given the lack of clarity about the standard, the determination at the school level, then, is left to the school. Meaning, then, that the determination for practical purposes is subjective.

34. N.H. REV. STAT. ANN. § 193-F:3(1) (2011).

35. ALA. CODE § 16-28B (2012); ARK. CODE ANN. § 6-18-514 (2009); COLO. REV. STAT. § 22-32-109.1 (2012); DEL. CODE ANN. tit. 14, § 4112D (Supp. 2012); GA. CODE ANN. § 20-2-751.4 (2012); IDAHO CODE ANN. § 18-917A (2006); 105 ILL. COMP. STAT. ANN. 5/27-23.7 (West 2012); IND. CODE ANN. § 20-33-8-0.2 (West Supp. 2014); IOWA CODE § 280.28 (2011); LA. REV. STAT. ANN. § 17:416.13 (Supp. 2014); MD. CODE ANN., EDUC. § 7-424 (West 2012); MICH. COMP. LAWS ANN. § 380.1310b (West 2013); MISS. CODE ANN. § 37-11-67 (Supp. 2013); MO. ANN. STAT. § 160.775 (West 2010); N.J. STAT. ANN. § 18A:37-14 (West 2013); N.C. GEN. STAT. § 115C-407.15 (2011); N.D. CENT. CODE § 15.1-19-17 (Supp. 2013); OHIO REV. CODE ANN. § 3313.666 (LexisNexis 2013); OKLA. STAT. tit. 70, § 24-100.3 (Supp. 2013); 24 PA. CONS. STAT. ANN. § 13-1303.1-A (West Supp. 2014); S.C. CODE ANN. § 59-63-120 (Supp. 2013); S.D. CODIFIED LAWS § 13-32-15 (Supp. 2013); TEX. EDUC. CODE ANN. § 37.0832 (West Supp. 2014); VT. STAT. ANN. tit. 16, § 11 (Supp. 2013); VA. CODE ANN. § 22.1-276.01 (Supp. 2014).

36. *E.g.*, DEL. CODE ANN. tit. 14, § 4112D(1) (Supp. 2012) (defining bullying as "any intentional written, electronic, verbal, or physical act or actions against another student").

37. CAL. EDUC. CODE § 48900(r) (West Supp. 2014); CONN. GEN. STAT. ANN. § 10-222d (Supp. 2014); FLA. STAT. ANN. § 1006.147 (West Supp. 2014); HAW. CODE R. § 8-19-2 (LexisNexis 2014); KAN. STAT. ANN. § 72-8256 (Supp. 2013); ME. REV. STAT. tit. 20-A, § 6554 (Supp. 2013); MASS. GEN. LAWS ch. 71, § 37O (West Supp. 2014); MINN. STAT. ANN. § 121A.0695 (West 2008); NEV. REV. STAT. § 388.123 (Supp. 2013); N.H. REV. STAT. ANN. § 193-F:3 (2011); N.M. Code R. § 6.12.7.7 (LexisNexis 2014); N.Y. EDUC. LAW § 11 (McKinney Supp. 2014); OR. REV. STAT. § 339.351 (2011); R.I. GEN. LAWS § 16-21-33

definitions provided by bullying laws, but they detail the various electronic means by which cyberbullying can happen.[38]

As noted in the Introduction, all of the states with cyberbullying laws authorize schools to monitor students' online and electronic activity. None, however, do so explicitly. Instead, they implicitly allow schools to engage in surveillance of students' online and electronic activity by authorizing or requiring that schools discipline students for electronic acts that constitute bullying.[39] To discipline for cyberbullying, the schools have to know whether it happens, and the cyberbullying laws are silent regarding how schools might go about discovering the prohibited conduct. Knowing whether cyberbullying is happening can be a tricky business. With more traditional physical or verbal bullying, as well as other discipline problems, schools typically know about it because either it occurs in front of a teacher or other school staff or students report incidents of it. The stereotypical bully, for example, might threaten a student in school and then physically assault the student behind the school after class lets out for the day. The fight could easily draw attention and noise, alerting school staff and allowing them to intervene. Even if school staff did not know about the bullying, they might likely see evidence of it in the physical bruises of the involved students.

Conversely, cyberbullying can easily occur without the school ever knowing about it, absent any student reporting, and the evidence of it is not very obvious or accessible. Unlike physical or verbal bullying, electronic acts cannot be readily seen or heard. Therefore, if a school is relying on the traditional means of knowing about student discipline issues—hearing or seeing them—the school will not know about the cyberbullying unless a student chooses to report it. Also unlike verbal or physical bullying, cyberbullying occurs in a nebulous time and space away from the eyes and ears of anyone other than the bully (or bullies) and the target. The time is nebulous because unlike in-person bullying, the electronic bullying message can be composed and sent at a time before, even significantly before, the target receives

(Supp. 2013); TENN. CODE ANN. § 49-6-4502 (2013); UTAH CODE ANN. § 53A-11a-102 (LexisNexis Supp. 2013).

38. *E.g.*, FLA. STAT. ANN. § 1006.147(3)(b) (West Supp. 2014) (defining cyberbullying as, among other things, "bullying through the use of technology or any electronic communication, which includes, but is not limited to, any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic system, photoelectronic system, or phototopical system, including, but not limited to, electronic mail, Internet communications, instant messages, or facsimile communications").

39. *E.g.*, South Carolina calls for "consequences and appropriate remedial actions for persons committing acts of . . . bullying." S.C. CODE ANN. § 59-63-140(B)(4) (Supp. 2013).

the message. The message can sit waiting in the target's e-mail inbox or on a smartphone or other electronic device for hours. Similarly, the space in which the bullying occurs is nebulous because the target can compose and send the bullying message from one location and the victim can receive it in a wholly different location. Indeed, even the physical location of the message can be unclear. Unlike some more traditional forms of bullying or harassment such as poison-pen letters, cyberbullying lacks tangibility. It exists somewhere, perhaps on a server somewhere, in the cloud, or elsewhere. The time and space in which the bullying occurs, therefore, is almost irrelevant to its impact. Regardless of where and when the bullying occurs, once the victim receives the message, its impact can be felt. Yet, the nebulous nature of its time and space occurrence does create difficulties for knowing about, accessing evidence of, and therefore addressing the bullying behavior. If a student sends a bullying message to another student at school, but the message is not received until the target is at home in the late hours of the night, the school may have difficulty both knowing it happened and administering the requisite discipline.[40]

One obvious way to overcome these difficulties and determine if students are engaged in cyberbullying is for schools, to the extent the cyberbullying laws allow it, to develop or acquire a system to monitor their students' online and electronic activity wherever and whenever it occurs. Since the cyberbullying laws do not prohibit such surveillance, the statutes implicitly allow the schools to monitor students' online and electronic activity, and schools, as discussed below, are starting to grab this implicit authority to conduct surveillance of all students' online and electronic activity.[41]

To an extent, schools' embrace of this implicit authority is understandable. Of the ways to determine if students are engaged in cyberbullying and therefore should be disciplined, a comprehensive surveillance system is probably the most effective and efficient means. Keeping electronic tabs on all students' online and electronic activity works to root out cyberbullying because it involves collecting information on all students' online and electronic activity, including any cyberbullying. It also therefore serves as the way to prevent a tragic suicide due to unaddressed cyberbullying.

To be sure, there are alternatives to this comprehensive surveillance method. Schools could confiscate all students' electronic devices to determine whether they are engaged in cyberbullying.

40. S.C. CODE ANN. § 59-63-140(B)(4) (Supp. 2013).

41. Schools often cannot discipline students under these laws without some impact of the bullying being felt at school, but they can nonetheless monitor students' online and electronic activity more broadly in an effort to determine if the activity creates the requisite discipline-invoking impact. *See infra* Part I.B.3.

Setting aside any potential Fourth Amendment problems with this method, this option is simply impractical in that it would require schools to review students' online and electronic activity one by one.[42] In addition to being impractical, the method would be only partially effective at best. With applications like Snapchat that can erase messages shortly after they are sent and received, confiscating the physical electronic devices may not result in schools' actually seeing and knowing about the bullying messages.[43]

Alternatively, schools could follow students on social media. Like the confiscation method, this method is similarly inefficient and likely ineffective.[44] It is inefficient because it would be difficult to know all the social media platforms on which to follow students, and it would be challenging at best to follow every student on all social media. It is also likely ineffective because students know when someone starts to follow them on social media.[45] The bully who makes any effort to not get caught could just choose a different form of social media—one on which he or she is not being followed by school staff—to carry out the bullying activity.

Schools could also just rely on the traditional method of student reporting. They could wait for students who are subjected to cyberbullying to inform them of the problem and then intervene. However, this option is similarly ineffective and inefficient if schools are working to really root out all cyberbullying.[46] Unless every student who experiences cyberbullying reports it to the school, the school will not be able to know about all the cyberbullying that is happening among its students. If one missed instance results in a suicide or suicide attempt, the school will face enormous criticism and scrutiny.

Instead, schools that are confronting these challenges head-on are opting for more global and efficient methods of monitoring of students' online and electronic activity when they have the authority to do so. As explained below, most of the states have this implicit authority, and some schools are therefore starting to employ

42. This is not to say that these Fourth Amendment concerns are insignificant. Indeed, the Supreme Court recently held that police searches of cell phones, even incident to arrest, require a warrant. *Riley v. California*, 134 S. Ct. 2473 (2014).

43. *Snapchat Guide for Parents*, SNAPCHAT http://www.snapchat.com/static_files/parents.pdf (May 1, 2014). Theoretically a school could still see an infringing Snapchat if the student screenshot the message before it disappeared.

44. *See* Thomas & Murphy, *supra* note 2; Sengupta, *supra* note 16.

45. *See, e.g.*, TWITTER, INC., *FAQs About Following*, https://support.twitter.com/articles/14019-faqs-about-following (last visited June 24, 2014).

46. *See supra* note 4 and accompanying text.

companies, such as Geo Listening and Safe Outlook Corporation, to conduct comprehensive surveillance of students.[47] According to the president of Geo Listening, Chris Frydrych, the company's service works by looking for "keywords and sentiments" on public posts by students.[48] Instead of providing a service, Safe Outlook Corporation sells a product called CompuGuardian, which allows for keyword searches of students' online activity.[49] David Jones, the president of Safe Outlook Corporation, was quoted as saying that by utilizing CompuGuardian, "you can identify a student, and you can jump into their activity logs and see exactly what they've typed, exactly where they've gone, exactly what they've done, and it gives you some history that you can go back to that child and use some disciplinary action."[50]

Not only are schools and school districts paying large sums for these services and products, but the companies also expect the sales and use of their products and services to grow. In 2013, Glendale School District in California paid Geo Listening more than $40,000 to monitor students' social media posts.[51] As of October 2013, at least two school districts and three schools were paying Safe Outlook Corporation between $1,000 and $9,000 per year for the use of its technology, and the company's president "expects the number of schools participating to go up."[52] Frydrych of Geo Listening expected to have 3,000 schools paying for his company's services by the end of 2013.[53]

### *B. Three Levels of Surveillance Authority*

In Glendale, California, the school district has interpreted its power under the cyberbullying statutes to allow it to conduct the surveillance it pays Geo Listening to do because the California cyberbullying statute implicitly authorizes surveillance of students.[54] Although the majority of cyberbullying statutes are like California's in that they implicitly authorize unlimited or nearly unlimited surveillance of students' online and electronic activity, not all states

47. *See* Sengupta, *supra* note 16; Wallace, *supra* note 16.

48. Sengupta, *supra* note 16.

49. Wallace, *supra* note 16.

50. *Id.*

51. *Id.*

52. *Id.*

53. Sengupta, *supra* note 16.

54. CAL. ED. CODE § 48900(r) (West Supp. 2014) (providing authority for schools to punish cyberbullying and therefore implicitly authorizing schools to monitor students' electronic activity to discover the prohibited electronic acts).

go so far. Some states require at least some nexus to school. While the use of this surveillance authority is very new, and the authority for it has not been plainly articulated or delineated, the clearest parameters for the implicit authority to monitor students' online and electronic activity lies in the authority to uncover cyberbullying behavior for which schools have the authority to discipline students. The nexus required by some states' laws is required in order to have authority to discipline. Although the cyberbullying laws' silence on the authority to conduct electronic surveillance of students leaves open the question of whether even more surveillance by schools is permitted, the schools' best argument that their surveillance is authorized lies in their need to uncover cyberbullying behavior for which they have the authority to then discipline students.

#### 1. Authorizing School Surveillance of Student Online and Electronic Activity If It Occurs at School or a Specific School-Related Event or Activity

Fifteen states require schools to have a substantial nexus to school in order to discipline students for cyberbullying.[55] These

55. These states are: Alabama, Iowa, Louisiana, Mississippi, Nebraska, Nevada, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, South Carolina, Texas, and Wyoming. ALA. CODE § 16-28B (2012); IOWA CODE § 280.28 (2011); LA. REV. STAT. ANN. § 17:416.13 (Supp. 2014); MISS. CODE ANN. § 37-11-67 (Supp. 2013); NEB. REV. STAT. § 79-2,137 (Supp. 2013); NEV. REV. STAT. § 388.135 (Supp. 2013); N.M. CODE R. § 6.12.7.7 (LexisNexis 2014); N.C. GEN. STAT. § 115C-407.15 (2011); N.D. CENT. CODE § 15.1-19-17 (Supp. 2013); OHIO REV. CODE ANN. § 3313.666 (LexisNexis 2013); OKLA. STAT. tit. 70, § 24-100.4 (Supp. 2013); OR. REV. STAT. § 339.351 (2011); S.C. CODE ANN. § 59-63-120(1)(a) (Supp. 2013); TEX. EDUC. CODE ANN. § 37.0832 (West Supp. 2014); WYO. STAT. ANN. § 21-4-312 (2011). Oregon also authorizes schools to discipline for cyberbullying if it happens on property adjacent to school property. OR. REV. STAT. § 339.351 (2011). An argument could be made that Louisiana falls into the "no nexus" category of states because it allows schools to discipline for cyberbullying and bullying "at a school-sponsored or school-related function or activity," which could include activities such as a student doing homework in her bedroom. LA. REV. STAT. ANN. § 17:416.13(C)(2)(a) (Supp. 2014). That said, the specificity with which the statutes delineate where students can be when schools have authority to discipline for bullying, including "on school property, at a school-sponsored or school-related function or activity, in any school bus or van, at any designated school bus stop, in any other school or private vehicle used to transport students to and from schools, or any school-sponsored activity or event," suggests the statute requires something more than virtually no nexus to school. *Id.* The same is also true for South Carolina's statute, which defines "school" (where bullying for which schools can discipline can happen) as "in a classroom, on school premises, on a school bus or other school-related vehicle, at an official school bus stop, at a school-sponsored activity or event whether or not it is held on school premises, or at another program or function where

"activity nexus" states authorize schools to discipline students for cyberbullying it if happens in school or when the students are physically on schoolhouse property.[56] In addition, some of these states provide schools with the authority to discipline students for cyberbullying if it happens outside the physical school building or off the physical property of the school but still at school-sponsored activities.[57] More specifically, several states allow schools to discipline for cyberbullying that happens on the school bus.[58] Several more states expressly allow schools to discipline for cyberbullying if it happens on any school or school-provided transportation, school bus or otherwise.[59] Certain states call on schools to discipline students for cyberbullying that happens at school bus stops.[60] One state, Louisiana, provides for student discipline if cyberbullying happens on the way to or from school no matter the type or ownership of the transportation used.[61] Nine states call on schools to discipline students for cyberbullying that happens at any school-sponsored or sanctioned events.[62]

Because schools in these activity nexus states cannot discipline students without that nexus, the schools have a relatively weak

---

the school is responsible for the child." S.C. CODE ANN. § 59-63-120(1)(a) (Supp. 2013).

56. *Id.*

57. *Id.*

58. *See e.g.*, ALA. CODE § 16-28B (2012); MISS. CODE ANN. § 37-11-67 (Supp. 2013); NEV. REV. STAT. § 388.135 (Supp. 2013); N.Y. EDUC. LAW § 11 (McKinney Supp. 2014); N.C. GEN. STAT. § 115C-407.15 (2011); OHIO REV. CODE ANN. § 3313.666 (LexisNexis 2013).

59. *See e.g.*, LA. REV. STAT. ANN. § 17:416.13 (Supp. 2014); NEB. REV. STAT. § 79-2,137 (Supp. 2013); N.M. CODE R. § 6.12.7.7 (LexisNexis 2014); N.D. CENT. CODE § 15.1-19-17 (Supp. 2013); OR. REV. STAT. § 339.351 (2011); S.C. CODE ANN. § 59-63-120 (Supp. 2013); TEX. EDUC. CODE ANN. § 37.0832 (West Supp. 2014); UTAH CODE ANN. § 53A-11a-201(2) (LexisNexis Supp. 2013); WYO. STAT. ANN. § 21-4-312 (2011).

60. *See e.g.*, N.M. Code R. § 6.12.7.7 (LexisNexis 2014); OR. REV. STAT. § 339.351 (2011); S.C. CODE ANN. § 59-63-120 (Supp. 2013); UTAH CODE ANN. § 53A-11a-201(2) (LexisNexis Supp. 2013).

61. LA. REV. STAT. ANN. § 14:40.7(C) (Supp. 2014) ("An offense committed pursuant to the provisions of this Section may be deemed to have been committed where the communication was originally sent, originally received, or originally viewed by any person.").

62. ALA. CODE § 16-28B (2012); LA. REV. STAT. ANN. § 14:40.7 (Supp. 2014); MISS. CODE ANN. § 37-11-67 (Supp. 2013); NEV. REV. STAT. § 388.123 (Supp. 2013); N.M. CODE R. § 6.12.7.7 (LexisNexis 2014); N.Y. EDUC. LAW § 11 (McKinney Supp. 2014); OHIO REV. CODE ANN. § 3313.666 (LexisNexis 2013); S.C. CODE ANN. § 59-63-120 (Supp. 2013); TEX. EDUC. CODE ANN. § 37.0832 (West Supp. 2014).

argument that they have authority to monitor students' online or electronic activity absent such a link. While a lack of any explicit authorization to conduct surveillance is not the same as a prohibition, the schools in these activity nexus states have no valid basis for conducting surveillance of students when they cannot discipline for the conduct they uncover. For example, if a student is at home using a smartphone in his or her bedroom, and the smartphone use has no relationship to school, the student cannot be disciplined at school for any online or electronic activity conducted at that time. Therefore, schools have no foundation for monitoring students to determine if that conduct warrants discipline.

New Mexico is an example of an activity nexus state. New Mexico's definition of bullying is contained in its administrative code. New Mexico Administrative Code Section 6.12.7.7 prohibits bullying, including bullying by "electronic expression." However, it limits its definition of bullying to that which occurs "in the school, on school grounds, in school vehicles, at a designated school bus top, or at school activities or sanctioned events."[63] Outside these activities, schools in New Mexico cannot discipline for cyberbullying and therefore have scant reason to conduct surveillance on students outside these contexts.

2. Authorizing School Surveillance of Students' Online and Electronic Activity If It Has a Nexus to School Equipment or Networks

In seven states, the cyberbullying statutes require a less substantial nexus to school in order to discipline for and therefore monitor students' online and electronic activity.[64] In these "ownership nexus" states, the schools can discipline students for cyberbullying if it is done using a school computer, school electronic equipment, a school network, or other school property.[65] Two of these states, Kansas and Rhode Island, prohibit cyberbullying through the use of any school property, which of course could include school computers or networks.[66] The rest prohibit cyberbullying if a student uses either school networks or equipment to do it.[67] In these states, if a student is

63. N.M. CODE R. § 6.12.7.7(A) (LexisNexis 2014).

64. These states are: Arizona, Delaware, Georgia, Illinois, Kansas, Michigan, and Rhode Island. ARIZ. REV. STAT. ANN. § 15-341 (2012); DEL. CODE ANN. tit. 14, § 4112D (2011); GA. CODE ANN. § 20-2-751.4 (West 2012); 105 ILL. COMP. STAT. ANN. 5/27-23.7 (West 2012); KAN. STAT. ANN. § 72-8256 (Supp. 2013); MICH. COMP. LAWS ANN. § 380.1310b (West 2014); R.I. GEN. LAWS § 16-21-33 (Supp. 2013).

65. *Id.*

66. KAN. STAT. ANN. § 72-8256 (Supp. 2013); R.I. GEN. LAWS § 16-21-33 (Supp. 2013).

67. ARIZ. REV. STAT. ANN. § 15-341 (2013); DEL. CODE ANN. tit. 14, § 4112D (2012); GA. CODE ANN. § 20-2-751.4 (2014); 105 ILL. COMP.

at home using a school-issued and -owned tablet to engage in cyberbullying, then the school can discipline for it. However, the school cannot discipline for cyberbullying if the student is at home but using a personal tablet or other device and a private network. Because the authority to discipline is so limited, the surveillance authority is too, at least implicitly. If a student is not using school equipment or a school network, the schools have no authority to discipline and therefore little to no authority to monitor students' online and electronic activity.

Illinois has such an ownership nexus statute.[68] In Illinois the definition of bullying and prohibition against it is contained in its statutory code. Illinois Compiled Statute Section 105-5/27-23.7 states that "[n]o student shall be subjected to bullying." It goes on to define cyberbullying as that which occurs "through the transmission of information from a school computer, a school computer network, or other similar electronic school equipment."[69] In Illinois, then, since the schools can only discipline for cyberbullying that occurs through the use of school equipment or networks, they have little, if any, legitimate basis for monitoring students' online and electronic activity when that activity is not conducted through the school equipment or networks.

While it might seem that the school equipment or network limitation on these schools' surveillance authority is significant, in actuality these states still authorize schools to conduct very broad surveillance of students that goes beyond the time and space of school itself. First, the schools could, if they were so inclined, conceivably go beyond the surveillance authority implicitly provided in these laws because the laws lack any mechanism for controlling schools' use of their authority. The laws have no cause of action or other device to hold schools accountable if schools exceed any implicit surveillance authority in the laws.[70] Therefore, if schools choose to monitor students' online and electronic activity conducted with school equipment or networks, and they choose or allow surveillance to bleed into student activity done without the use of school equipment or networks, students have little, if any, means to stop them.[71]

---

STAT. 5/27-23.7 (West 2012); MICH. COMP. LAWS ANN. § 380.1310b (West 2013).

68. 105 ILL. COMP. STAT. 5/27-23.7(a) (West 2012).

69. 105 ILL. COMP. STAT. 5/27-23.7(a)(3) (West 2012).

70. *See infra* Part III.B.3.

71. Of course, this is true of most statutes providing the state with authority but not offering enforcement mechanisms when the state exceeds that authority. Thus, the need exists for a cause of action to limit the misuse of state authority. *See infra* Part IV.A.

Also, if a student chooses to engage in online or electronic activity at home and after school but uses school equipment or networks to do it, then the school can still monitor the student's online and electronic activity even though it occurs in a time and space beyond the school and school day. While it is true that students could circumvent a school's surveillance authority by using their own equipment and networks, for some students this circumvention is not so easy or simple. Consider low-income students. They are less likely than high-income students to own a computer and much less likely to own a tablet.[72] So while students from high-income families can escape school surveillance by using their own equipment or networks, low-income students cannot so readily escape it. The ownership nexus limitation on the schools' surveillance authority, therefore, really only protects privileged students who need not rely on school equipment to access electronic data.

In addition, given that the student population in the public schools is increasingly low-income, the ownership nexus is increasingly less of a limitation on school surveillance authority.[73] In seventeen states the majority of students in public schools are low-income, and for them, it is likely that school equipment and networks are their only regular access to certain electronic data and equipment.[74] Indeed, many schools, in part out of recognition of these changing demographics, are giving out technology to students, including equipment like iPads, as additional learning tools.[75] As a result,

72. In the lowest income households (those earning less than $30,000 per year), only 73 percent own a computer versus 81 percent of the highest income households (those earning more than $75,000 per year) owning a computer. Mary Madden et al., *Teens and Technology 2013*, PEW RESEARCH INTERNET PROJECT at 6 (Mar. 13, 2013), http://www.pewinternet.org/2013/03/13/main-findings-5/. Income is very predictive of owning a tablet, with only 15 percent of teens in the lowest income households compared to 31 percent of teens in the highest income households owning a tablet. *Id.*

73. Steven Suitts, *A New Majority: Low Income Students in the South and Nation*, SOUTHERN EDUCATION FUND 8 (Oct. 2013), http://www.southerneducation.org/getattachment/0bc70ce1-d375-4ff6-8340-f9b3452ee088/A-New-Majority-Low-Income-Students-in-the-South-an.aspx (providing statistics suggesting an increase in the number of low-income students).

74. *Id.* at 2 tbl.1 (listing states with "a majority of low income students in public schools" in 2011).

75. The Los Angeles Unified School District has famously given out iPads to all of its students, and other school systems from Ohio to Alabama have done the same. Howard Blume & Steven Ceasar, *As Schools Give Students Computers, Price of L.A.'s Program Stands Out*, L.A. TIMES, Dec. 31, 2013, *available at* http://www.latimes.com/local/la-me-ipads-schools-20140101-story.html#page=1.

students in ownership nexus states who do not have a personal tablet device to use at home, but who want to become familiar with this increasingly common technology,[76] will potentially be subjected to surveillance. To be fair, schools need some authority to control their own equipment, but this authority does not require the broadening of surveillance authority. Schools have already abused this authority to control their own equipment by committing serious intrusions into student privacy, including watching students in their homes and bedrooms through webcams in school-owned equipment.[77] Instead, schools should employ available means other than comprehensive surveillance to control their devices. Schools, for example, can block websites and the ability of students to download applications onto the devices.[78]

Finally, expecting students to forego technology in order to avoid surveillance by schools is unrealistic and denies the allure technology has for young people. In their book *Liquid Surveillance*,[79] Zygmunt Bauman and David Lyon discuss the concept they call "liquid surveillance." Among other things, Bauman and Lyon conceive of liquid surveillance as a fluid way of thinking of surveillance.[80] The authors point to the fluidity of surveillance in the consumer world, where consumption is the result of "the pleasurable seduction of consumers."[81] They argue that people submit to surveillance and the attendant "loss of privacy as a reasonable price for the wonders offered in exchange."[82] An example of such submission is the loyalty cards that offer discounts at grocery stores.[83] Bauman & Lyon cite an

76. According to a 2012 study by the Pew Research Center, 95 percent of teens are online, and 78 percent have a cell phone of some kind. *See* Madden et al., *supra* note 72, at 2–3.

77. For example, in Pennsylvania, students accused a school official of activating web cameras on school-owned laptops to watch students while they were at home. *See* Clarke, *supra* note 17.

78. While this solution has not always been perfect, as evidenced by Los Angeles Unified School District's initial iPad rollout in which students got beyond the security controls quickly, the controls ultimately get fixed. Howard Blume, *LAUSD Halts Home Use of iPads for Students After Devices Hacked*, L.A. TIMES, Sept. 25, 2013, *available at* http://articles.latimes.com/2013/sep/25/local/la-me-ln-lausd-ipad-hack-20130925.

79. ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE 2 (2013).

80. *Id.* at 4–5.

81. *Id.* at 121.

82. Zygmunt Bauman, *On Never Being Alone Again*, SOCIAL EUROPE J. June 28, 2011, http://www.social-europe.eu/2011/06/on-never-being-alone-again/.

83. BAUMAN & LYON, *supra* note 79 at 128 (internal citation omitted).

international study that found people "'either don't know or don't care' about the connections between the use of loyalty cards and profiling."[84] People submit to the surveillance to get the benefits of the loyalty cards.[85] It is reasonable to expect that surveillance of students by schools through school equipment and networks is similarly liquid. Surveillance is liquid in the sense that it is hard for students to turn down technology's wonders in the name of privacy or security. This is probably especially true for low-income students. Even if the students could turn down equipment like school-issued tablets (and they may not be able to if their schoolwork must be done on a tablet) in order to forego surveillance, it would be expecting a lot of students to make that decision. Students live in a technology driven world where they are more likely to submit to the lures of technology, like free laptops and iPads from their school, than to sacrifice this equipment in the name of increased privacy.[86] To dismiss the surveillance authorized in these seven ownership nexus states under cyberbullying statutes as optional, then, is to ignore the strength of the technology's appeal and the ubiquity of its use.

3. Authorizing School Surveillance of Student Electronic Activity Without Any Nexus to the School or School-Related Activities

Twenty-three states and the District of Columbia have statutes that allow for virtually unlimited surveillance of students' online and electronic activity.[87] These "zero nexus" laws implicitly authorize

84. *Id.*

85. *Id.*

86. *See* CBSNEWS, *$610K Settlement in School Webcam Spy Case* (Oct. 21, 2010), http://www.cbsnews.com/news/610k-settlement-in-school-webcam-spy-case/ (noting that even after catching school officials using his webcam to view activities within his bedroom, the spied-upon Harrington High School student "says his computer behaviors haven't changed much . . . .").

87. These states are Arkansas, California, Colorado, Connecticut, Florida, Hawaii, Idaho, Indiana, Maine, Maryland, Massachusetts, Minnesota, Missouri, New Hampshire, New Jersey, New York, Pennsylvania, South Dakota, Tennessee, Utah, Vermont, Washington, West Virginia, and the District of Columbia. ARK. CODE ANN. § 6-18-514 (2009); CAL. EDUC. CODE § 48900 (West Supp. 2014); COLO. REV. STAT. § 22-32-109.1 (2012); CONN. GEN. STAT. ANN. § 10-222d(b)(16) (2010); FLA. STAT. ANN. § 1006.147 (West Supp. 2014); HAW. CODE R. § 8-19-2( (LexisNexis 2014); IDAHO CODE ANN. § 18-917A (2006); IND. CODE ANN. § 20-33-8-0.2 (West Supp. 2014); ME. REV. STAT. TIT. 20-A, § 6554 (Supp. 2013); MD. CODE ANN., EDUC. § 7-424 (West 2012); MASS. GEN. LAWS ANN. CH. 71, § 37O (West Supp. 2014); MINN. STAT. ANN. §§ 121A.0695, 121A.031 (West 2008); MO. ANN. STAT. § 160.775 (West 2010); N.H. REV. STAT. ANN. § 193-F:4 (2011); N.J. STAT. ANN. § 18A:37-14 (West 2014); N.Y. EDUC. LAW § 11 (McKinney Supp. 2014); 24 PA. CONS. STAT. ANN. § 13-1303.1-A(d)

schools to monitor students' online and electronic activity regardless of where or when it is conducted. For example, California's statute prohibits bullying by "electronic act," which act serves as grounds for suspension or expulsion of the student when it occurs.[88] While the statute discusses the acts of bullying in relation to school activities and attendance, in reality there is no limit in the statute on where or when the bullying can occur.[89] Because schools have the authority to punish bullying that occurs anywhere and at any time by electronic act, they implicitly have the authority to search for and discover it whenever and wherever it occurs.[90] This interpretation provides the authority for Glendale School District's use of Geo Listening to conduct comprehensive surveillance of all of its students' online and electronic activity.[91]

Other states are even more liberal than California in the broad grant of authority to schools to punish, and therefore monitor, students' online and electronic activity. Indiana and New York are two such states that exhibit the breadth of school authority.[92] Indiana prohibits bullying, including cyberbullying, by students "regardless of the physical location in which the bullying behavior occur[s]."[93] New York defines bullying, including cyberbullying, to consist of certain activity that occurs "off school property."[94] Although the New York

(West Supp. 2014); S.D. CODIFIED LAWS § 13-32-15 (Supp. 2013); TENN. CODE ANN. § 49-6-4502 (Supp. 2013); UTAH CODE ANN. § 53A-11a-201(2) (LexisNexis Supp. 2013); VT. STAT. ANN. TIT. 16, § 11(a)(32)(C)(ii) (Supp. 2013); WASH. REV. CODE § 28A.300.285 (2012); W. VA. CODE § 18-2C-2 (LexisNexis 2012); D.C. CODE §§ 2-1535.01 to 2-1535.09.

88. CAL. EDUC. CODE § 48900(r) (West Supp. 2014).

89. *Id.* The subsequent provision requires the acts enumerated in the section to be "related to a school activity or school attendance" before discipline can be ordered. § 48900(s) (West Supp. 2014). However, many electronic activities can occur off school grounds and still be related to school activity. *See, e.g.*, *infra* note 122 and accompanying text. Moreover, the same provision specifically notes that the disciplinable act may occur "at any time" § 48900(s) (West Supp. 2014). The provision goes on to list periods where this activity may occur, all of which are tied to the school's campus, the school day, or travel to and from a school-sponsored activity. *Id.* However, the text explicitly notes that this list is inexhaustive. *Id.*

90. *See* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. ON TELECOMMS. & HIGH TECH. L. 357 (2011) (explaining why common law privacy torts have limited utility for redressing surveillance in the digital age).

91. *See supra* Part I.A.

92. IND. CODE ANN. § 20-33-8-0.2 (West Supp. 2014); N.Y. EDUC. LAW § 11(7) (McKinney Supp. 2014).

93. IND. CODE ANN. § 20-33-8-13.5(b) (West Supp. 2014).

94. N.Y. EDUC. LAW § 11(7) (McKinney Supp. 2014).

statute, like many but certainly not all,[95] goes on to qualify the definition so that the off-campus bullying has to "create or foreseeably create a risk of substantial disruption within the school environment, where it is foreseeable that the conduct, threats, intimidation, or abuse might reach school property," this qualification does nothing to limit the surveillance authority of the school.[96] While schools in New York cannot discipline for bullying that they learn about if it occurs off campus and creates no risk of substantial disruption or the threats reaching the school, they can still monitor students' online and electronic activity occurring off-campus to *determine* if they can and should discipline students. Again, as with the cyberbullying statutes more generally, surveillance allows schools to know about the activity for which they may need to discipline students regardless of whether they actually will have the authority to discipline for it.

What can this enormous level of surveillance authority mean for students? Imagine that two teenage, female students who attend the same school get into an argument during summer break. The argument takes place entirely over text and social media apps on the students' smart phones. The argument has nothing to do with school, and it occurs during non-school, summer break hours. The messages the girls send and receive are only sent to and received from their homes and other non-school locations. Because their school district has CompuGuardian, however, it learns of the argument as well as much or all of the other information the students have posted electronically, irrespective of its relationship to school or bullying. Through CompuGuardian, school staff members are alerted to messages sent by one of the girls that could be misinterpreted as cyberbullying. Although the girls resolve their argument and are friends again by the time school resumes after summer break, the girl who sent the misinterpreted message is suspended on the first day of school for cyberbullying. The school's position is that the discipline is warranted because the summer argument could disrupt the school. In addition to the discipline, both girls are now acutely aware that the school is monitoring their electronic communications, and they start

95. California's statute, for example, does not require that the electronic bullying have an impact at school in order to subject the bully to discipline. By authorizing schools to discipline students for electronic acts, without limitation on where or when they occur, it allows California to monitor all students' electronic acts. If those acts, for example, "can be reasonably predicted to have the effect of . . . placing a reasonable pupil . . . in fear of harm to that pupil's . . . person or property," then the school can suspend or expel the bully, regardless of where the electronic act took place or where the student was when in fear of harm to her person or property. CAL. EDUC. CODE § 48900(r) (West Supp. 2014); *see also supra* note 89 and accompanying text.

96. N.Y. EDUC. LAW § 11(7) (McKinney Supp. 2014).

limiting what they say about anything the school could uncover and object to, including messages about schoolwork. In this easily imagined hypothetical case, the school surveillance authority reaches beyond school space and time. It results both in the suspension of a girl for actions that she and her friend have since resolved and the school's collecting large amounts of data on these and other students, much of which has nothing to do with school or bullying.

## II. AN UNPRECEDENTED EXPANSION OF SCHOOL AUTHORITY

Given the novelty of school authority under cyberbullying laws to conduct surveillance of students' online and electronic activity, it is not surprising that there is no doctrine on point regarding its limits. Thus, understanding how school surveillance authority reflects an expansion of traditional limits on school authority requires looking to other doctrinal restrictions on school authority to get a sense of where courts have been willing to draw boundaries. Overarching constitutional limits on school authority derive from First and Fourth Amendment student-speech and search doctrines. While school surveillance authority does not fit squarely into either the First or Fourth Amendment school doctrine, it touches on elements of both, thus providing relevant guidance on the limits of school authority. More generally, Supreme Court doctrine on government surveillance provides some guideposts to assess the limits of state and therefore school surveillance authority.

### *A. The Limits of School Authority Under First Amendment Doctrine*

#### 1. Schools' Expanded Authority to Regulate Student Speech

Schools generally have more authority than state actors under the Constitution to regulate student speech. That authority in some circumstances extends beyond the physical boundaries of the school. Thus, First Amendment doctrine offers insight into where the courts have been willing to draw lines regarding school authority. In *Tinker v. Des Moines Independent Community School District*,[97] the Supreme Court articulated both a willingness to protect student speech in school and recognized that students' First Amendment rights in school are not coextensive with those rights in other contexts. The students in *Tinker* were disciplined for wearing black armbands to school in protest of the Vietnam War.[98] They challenged the disciplinary action on First Amendment grounds.[99] Famously pronouncing that students do not "shed their constitutional rights to

97. Tinker v. Des Moines Indep. Sch. Dist., 393 U.S. 503 (1969).

98. *Id.* at 504.

99. *Id.* at 505.

freedom of speech or expression at the schoolhouse gate,"[100] the Court went on to find that student speech may nonetheless be limited if it "materially disrupts classwork or involves substantial disorder or invasion of the rights of others."[101] Finding no such disruption, disorder, or invasion, the Court overturned the school disciplinary action as a violation of the First Amendment.[102]

Because the students in *Tinker* wore their armbands in the school building, the standard articulated in that case for limiting student speech a material and substantial disruption or invasion of the rights of others—applies in that specific setting. *Tinker* did not have cause to address where the boundaries of "in school" begin and end. Therefore, while a school's increased authority to impinge on students' free-speech rights may or may not extend beyond the schoolhouse gate, *Tinker* did not decide that issue.[103]

Other Supreme Court cases on student speech have done little to clarify the physical or temporal boundaries of school authority. In *Bethel School District v. Fraser*,[104] the Supreme Court found that schools have an increased authority, as compared to other state actors, to regulate students who make lewd speech in school.[105] In *Fraser*, a student was disciplined for making a vulgar speech at a school assembly.[106] In finding that the school could regulate the speech, and therefore discipline the student, the Court again did not have reason to define where the boundaries of "in school" begin and end. As in *Tinker*, the student in question made the lewd speech in school,[107] and the holding was limited to those narrow facts. Though *Fraser* did not address the physical boundaries associated with this increased authority to regulate student speech, *Morse v. Frederick*[108] later clarified that the authority to regulate students' lewd speech was

100. *Id.* at 506.

101. *Id.* at 513. The *Tinker* opinion also indicated that student speech "'materially and substantially interfere[s] with the requirements of appropriate discipline in the operation of the school, . . . .'" *Id.* at 509 (quoting Burnside v. Byars, 363 F.2d 744, 749 (5th Cir. 1966)).

102. *Id.* at 514.

103. Doninger v. Niehoff, 527 F.3d 41, 48 (2d Cir. 2008) ("The Supreme Court has yet to speak on the scope of a school's authority to regulate expression that . . . does not occur on school grounds or at a school-sponsored event.").

104. Bethel Sch. Dist. v. Fraser, 478 U.S. 675 (1986).

105. *Id.* at 685.

106. *Id.* at 677 78.

107. *Id.*

108. Morse v. Frederick, 551 U.S. 393 (2007).

limited to the physical school setting.[109] In *Morse*, the majority stated that "[h]ad Fraser delivered the same speech outside the school context, it would have been protected."[110]

*Morse* and an earlier case, *Hazelwood School District v. Kuhlmeier*,[111] identified some specific kinds of speech that can be regulated by the school regardless of whether the speech physically occurs within the school setting. In *Kuhlmeier*, the Court considered speech made by students in a school newspaper.[112] It concluded that schools generally have more authority than the state does to regulate school-sponsored student speech—such as speech made through a student newspaper.[113] In *Morse v. Frederick*, more famously known as the "Bong Hits 4 Jesus" case, the Court considered whether a sign held up by a student at an off-campus, school-sponsored activity that could be interpreted to support illegal drug use could be regulated by the school.[114] It concluded that drug-supporting speech at school-sponsored activities, off-campus or not, can be regulated by schools.[115] For school-sponsored speech and drug-supporting speech at school-sponsored activities, the school boundaries are broader than the school boundaries for lewd speech: they extend beyond the physical location of the school.

Since *Fraser*, *Kuhlmeier*, and *Morse* apply specifically to lewd speech, school-sponsored speech, and drug-supporting speech at school-sponsored activities, they do not determine the boundaries of school authority in other contexts most relevantly when the school is conducting surveillance of students' online and electronic activity outside the school. The federal appellate courts have therefore been left to grapple with applying the *Tinker* standard to address discipline of students' online speech when it does not occur in the school building or at a school-related or sponsored event.[116] The Circuits have developed two different standards for evaluating the extent of school authority to discipline students for speech that occurs online and off-campus. One line of cases from the Second,[117] Third,[118] and

109. *Id.* 405.

110. *Id.*

111. Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260 (1988).

112. *Id.* at 262.

113. *Id.* at 273.

114. *Morse*, 551 U.S. at 397.

115. *Id.* at 410.

116. Doninger v. Niehoff, 642 F.3d 334, 346 (2d Cir. 2011) (applying the *Tinker* standard to school discipline of online student activity that occurred off school property).

117. Wisniewski v. Bd. of Educ., 494 F.3d 34, 39 (2d Cir. 2007) (regarding a student's online instant message).

Eighth[119] Circuits use essentially the *Tinker* standard or a variation of it. The Second Circuit has articulated its test as one that permits schools to regulate what might otherwise be protected speech made online and off-campus if the speech poses a reasonably foreseeable risk that it will both "come to the attention of school authorities and that it would 'materially and substantially disrupt the work and discipline of the school.'"[120] If the student speech meets this test, then the boundaries of the school extend beyond campus to virtually any place the speech occurs. The Second Circuit, in *Doninger v. Niehoff*,[121] found such a reasonably foreseeable risk when a student made a blog post at home, and the blog was hosted on a website wholly unaffiliated with school.[122] The Court found that the blog post, which invited students to protest the school superintendent's decision regarding the date and location of a school jam fest music event, "directly pertained to an event" at school and "invited other students to read and respond to it by contacting school officials."[123] Thus, the Court concluded that it was reasonably foreseeable that the post would "reach school property and have disruptive consequences there."[124]

The Fourth Circuit has a somewhat different approach for the standard for determining the breadth of school authority to regulate students' off-campus and online speech. In *Kowalski v. Berkeley County Schools*,[125] a student created a MySpace page that was "largely dedicated to ridiculing a fellow student."[126] The student who

118. J.S. v. Blue Mountain Sch. Dist., 650 F.3d 915, 931 (3d Cir. 2011) (finding that a student who was suspended for creating a MySpace page about her school principal on the weekend using her home computer could not be disciplined without violating the First Amendment).

119. S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771, 777 (8th Cir. 2012) (holding that where a student's blog post was made at home and on a platform unaffiliated with the school, the "student speech that causes a substantial disruption is not protected").

120. *Wisniewski*, 494 F.3d at 38–39.

121. *Doninger*, 642 F.3d at 344.

122. *Id.* at 348.

123. *Id.*

124. *Id.* As with the statutes that do not specify whether the determination of the impact on school is subjective or objective, the court did not clarify whether the assessment of the "disruptive consequences" at school would be subjective or objective. *Id.* Again, given that the determination is then largely left to the school at the school level by school staff, it is for practical purposes a subjective determination made by those school staff members. *See supra* note 31 and accompanying text.

125. Kowalski v. Berkeley Cnty. Schs., 652 F.3d 565 (4th Cir. 2011).

126. *Id.* at 567.

created the MySpace page was suspended from school for five days and challenged the suspension on First Amendment grounds.[127] The Court concluded that the school could regulate student off-campus and online speech if the nexus between the speech and the school's pedagogical interests was sufficiently strong to justify the disciplinary action regulating the speech.[128] In *Kowalski*, the Court found that the nexus requirement could be met by the material or substantial disruption test because although the MySpace page was created at home, the student "knew that the electronic response would be, as it in fact was, published beyond her home and could reasonably be expected to reach the school or impact the school environment."[129] Although acknowledging that there is "a limit to the scope of a high school's interest in the order, safety, and well-being of its students when the speech at issue originates outside the schoolhouse gate," the Court declined to define that limit.[130] It instead limited itself to finding that the student's speech on the MySpace page had a sufficiently strong nexus to those pedagogical interests.[131]

In sum, schools' authority to regulate student speech is broader than that of other state actors and at times can extend beyond the physical boundaries of schools. Supreme Court cases indicate that schools can regulate student speech even if it occurs off-campus if it is school-sponsored speech or if it is drug-supporting speech made at a school-sponsored activity.[132] In addition, in some Circuits, if there is a "reasonably foreseeable risk that the [speech will] come to the attention of school authorities" and create a material and substantial disruption in school,[133] or if the regulation of the speech has a sufficiently strong nexus to a school's pedagogical interests,[134] then student speech may be regulated by schools regardless of where and when it occurs.

### 2. If Increased School Authority to Regulate Student Speech Is a Guide, Cyberbullying Laws Expand School Authority

Although the limits on school authority under student-speech cases provide a rough guide for the general limits on school authority,

127. *Id.* The student additionally brought a challenge on Fourteenth Amendment grounds. *Id.*

128. *Id.* at 573.

129. *Id.*

130. *Id.*

131. *Id.*

132. Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260, 273 (1988); Morse v. Frederick, 551 U.S. 393, 410 (2007).

133. Wisniewski v. Bd. of Educ., 494 F.3d 34, 38 (2d Cir. 2007).

134. *Kowalski*, 652 F.3d at 573.

the surveillance authority of schools under cyberbullying statutes exceeds those limits. Because of its sweeping nature, the surveillance of all of students' online and electronic activity whenever and wherever it occurs under cyberbullying statutes gathers information about students that has nothing to do with any foreseeable risk of a material or substantial disruption in school or any nexus to pedagogical interests.[135] The surveillance authority instead allows schools to learn any information about students that is posted online or electronically regardless of whether it has to do with school at all.[136] Accordingly, schools have the authority under the majority of cyberbullying statutes to obtain information about students regardless of its connection to school.[137]

Of course, surveillance of students under cyberbullying statutes is distinct from the student-speech cases in one way. The student-speech cases focus on the regulation of student speech by means of school discipline.[138] The surveillance of students under cyberbullying statutes happens before the student discipline takes place. In that sense, the First Amendment cases seem at least somewhat inapposite. No speech has yet been regulated. Yet the student-speech cases still suggest where school authority begins and ends and, therefore, give an indication of how much cyberbullying laws expand that authority by allowing schools to conduct surveillance of students well beyond the time and space of school.

135. *See supra* Parts I.A, I.B.2, and I.B.3.

136. *Id.*

137. For a discussion of how a school could draft a cyberbullying policy that complies with First Amendment doctrine, see Goodno, *supra* note 4.

138. *E.g.*, Tinker v. Des Moines Indep. Sch. Dist., 393 U.S. 503 (1969) (noting how student was suspended for wearing armband); Bethel Sch. Dist. v. Fraser, 478 U.S. 675 (1986) (noting how student was suspended for sexual innuendo–filled speech); Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260 (1988) (noting how student articles on pregnancy and divorce were excluded from school newspaper); Morse v. Frederick, 551 U.S. 393 (2007) (noting how student suspended for "Bong Hits 4 Jesus" banner at school assembly); Wisniewski v. Bd. of Educ., 494 F.3d 34, 39 (2d Cir. 2007) (noting how student suspended for "creating and transmitting drawing depicting shooting of teacher"); Doninger v. Niehoff, 642 F.3d 334 (2d Cir. 2011) (noting how student excluded from election for protest against rescheduling of "Jamfest" event); Kowalski v. Berkeley County. Sch., 652 F.3d 565 (4th Cir. 2011) (noting how student suspended for posting to a webpage ridiculing another student); S.J.W. v Lee's Summit R-7 Sch. Dist., 696 F.3d 771, 773 74 (8th Cir. 2012) (noting how students suspended for "creating website with blog containing variety of offensive, racist, and sexist comments about school and classmates").

### *B. The Limits of School Authority Under Fourth Amendment Doctrine*

#### 1. Schools' Authority to Search Students in School

Schools' surveillance authority under the majority of cyberbullying statutes may seem something more akin to the authority to search students, which is subject to the limits of the Fourth Amendment. While, as with First Amendment doctrine, school surveillance authority does not fit neatly into current Fourth Amendment doctrine, it is nonetheless instructive as to the general limits of school authority. Here too, the surveillance authority exceeds even the expanded search authority provided to schools under the Fourth Amendment.

The seminal case on schools' authority to conduct student searches is *New Jersey v. T.L.O.*[139] In *T.L.O.*, a school assistant vice principal conducted an in-school search of a female student's purse on the suspicion that she was smoking in school, thus violating school rules.[140] The search uncovered marijuana and related paraphernalia, and the girl subsequently faced delinquency charges.[141] She sought to suppress the evidence of the search on Fourth Amendment grounds.[142] Finding that the Fourth Amendment's "prohibition on unreasonable searches and seizures applies to searches conducted by public school officials," the Supreme Court nonetheless upheld the validity of the search.[143] The Court held that, unlike in other contexts, school officials need neither a warrant nor probable cause to conduct a search of students in school.[144] Rather, searches of students in school need only be reasonable, as determined through application of a two-factor analysis.[145] First, a court must "consider 'whether the . . . action was justified from its inception.'"[146] Second, a court has to assess whether "the search as actually conducted 'was reasonably

139. N.J. v. T.L.O., 469 U.S. 325 (1985). The lower federal courts have heard Fourth Amendment cases in which students challenged searches of their online activity. When they have been presented with such cases, the courts analyze them under the *T.L.O.* framework. *E.g.*, R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128 (D. Minn. 2012) (assessing the search of a student's Facebook and e-mail accounts after she involuntarily gave school officials her login information under the *T.L.O.* standard and finding the search to have violated that standard).

140. *T.L.O.*, 467 U.S. at 328.

141. *Id.* at 328–29.

142. *Id.* at 329.

143. *Id.* at 333.

144. *Id.* at 340–41.

145. *Id.* at 341.

146. *Id.*

related in scope to the circumstances which justified the interference in the first place.'"[147] Finding the search of T.L.O. to meet both prongs of the test, the Court concluded that it met constitutional strictures.[148]

Following *T.L.O.*, the Supreme Court took up the question of whether schools could conduct suspicionless drug searches in *Vernonia School District v. Acton*.[149] In *Acton*, the Court considered the claim of a student, James Acton, who wanted to sign up to play football but refused to consent to school-administered and school-required drug testing in order to do it.[150] He challenged the drug-testing requirement on Fourth Amendment grounds.[151] The Court again applied a reasonableness standard, but it did not use the two-part test from *T.L.O.*[152] It upheld the drug testing program as reasonable because it found that (1) students have a reduced expectation of privacy in school and particularly in sports programs; (2) the requisite search was limited to drug testing (as opposed to also including things like pregnancy testing); and (3) testing is needed due to the widespread school drug problem and related discipline problems.[153]

### 2. If Increased School Authority to Search Student Speech Is a Guide, Cyberbullying Laws Expand School Authority

Although they do not precisely cover surveillance under cyberbullying laws, *T.L.O.* and *Acton* outline some of the limits on a school's search authority. Both limit school searches to those that are reasonable. The broad sweep of schools' surveillance authority under cyberbullying statutes, though, largely defies this standard. Take the two-factor test set forth in *T.L.O.* for determining reasonableness;[154] assuming school surveillance is a search, schools' surveillance of student online and electronic activity fails that two-factor test. First, the school authority fails the requirement that a search be "justified at its inception."[155] The broad surveillance authority provided by the cyberbullying laws has no justification other than an undifferentiated understanding that cyberbullying does happen sometimes among some students. This vague rationale for conducting surveillance of all

147. *Id.*

148. *Id.* at 345–47.

149. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 648 (1995).

150. *Id.* at 651.

151. *Id.*

152. *See id.* at 652.

153. *Id.* at 657–58, 661.

154. N.J. v. T.L.O., 469 U.S. 325, 341 (1985).

155. *Id.*

students without any specific suspicion attached cannot be considered legitimate justification. Second, the surveillance authority under the cyberbullying laws cannot be deemed reasonably related in scope to the initial justification. As already noted, the surveillance authority can occur without anything but the most amorphous of justifications. In addition, the scope, which allows schools to monitor all students at all times, could not be broader. To justify this scope, schools would have to suspect that all students are engaged in cyberbullying at all times.[156]

Similarly, the cyberbullying laws arguably fail to satisfy the metric for reasonableness articulated in *Acton*. *Acton* requires that in order for suspicionless, in-school student searches to be reasonable, they need to be limited in scope, among other things. Schools' surveillance of students under cyberbullying laws, however, can uncover vast amounts of information communicated online and electronically by students—not just information on cyberbullying. As such, the surveillance arguably defies the strictures of limitedness that support a conclusion that a search is reasonable.

That said, student search doctrine both in *T.L.O.* as well as in *Acton* still does not provide perfect guidance for interpreting the limits of school surveillance authority for at least three reasons. First, *T.L.O.* as well as *Acton* address searches that happen in school. In *T.L.O.*, the suspected violation of school rules and the consequent search conducted by the assistant vice principal both happened in the school building.[157] In *Acton*, the search of James Acton would have occurred in school had he consented to it.[158] The Supreme Court did not then, and has not subsequently, addressed whether schools have any authority to search students outside the time and space of the physical school setting or any limits thereof. Because surveillance under cyberbullying laws happens outside school, whether and how the Fourth Amendment doctrine under *T.L.O.* and *Acton* applies is an open question.

Second, Fourth Amendment doctrine on searches is invoked in order to suppress the evidence of the search when discipline (or prosecution) is imposed, or when other benefits or privileges are denied because of searches.[159] The school surveillance of students'

156. *See id.* at 341. For a discussion of how schools could have the authority to search students' electronic devices upon suspicion that cyberbullying was occurring in school during school hours, see Goodno, *supra* note 4.

157. *T.L.O.*, 469 U.S. at 328.

158. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 650 (1995).

159. Students may be entitled to some redress for Fourth Amendment violations without harm, but the damages they can recover would likely be only nominal. *See* G.C. v. Owensboro Pub. Schs., 711 F.3d 623, 634 (6th Cir. 2013).

online activity and the searches in *T.L.O.* and *Acton* either resulted in the discipline or the prosecution of a student, as in *T.L.O.*, or were limited to when a student had volunteered for specific school activities, as in *Acton*.[160] Electronic surveillance under cyberbullying laws can happen without any consequent discipline, prosecution, or denial of benefits or privileges. Whether the Fourth Amendment would provide redress for student surveillance without actual discipline or denial of privileges, then, is also an open question.[161] Therefore, the Fourth Amendment doctrine under *T.L.O.* and *Acton* does not provide precise bounds for the limits of school surveillance of students' online and electronic activity.[162]

Third, in order for the Fourth Amendment to be implicated, students must have a reasonable expectation of privacy in the object of the search.[163] Whether students have a reasonable expectation of privacy in many online and electronic communications is at best questionable.[164] Frequently used online tools and services like Google make clear that users' expectation of privacy in their searches and posts is limited.[165]

Despite these limitations on *T.L.O.* and *Acton* as guidelines for the confines of school surveillance authority, they nonetheless demonstrate, more generally, some of the bounds on school authority. Like student-speech cases, they offer insight into the outer limits of the authority of schools to search student in school and impose consequences as a result. Notwithstanding that school surveillance under cyberbullying laws occurs outside school (as well as inside) and potentially without the consequences of prosecution or the denial of privileges, it exceeds the kinds of limits set by the Fourth Amendment. It allows for the unjustified collection of potentially vast amounts of information communicated by students electronically at

160. T.L.O., 469 U.S. at 329; *Vernonia Sch. Dist.* 47J, 515 U.S. at 650.

161. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013) (failing to reach the issue of whether surveillance alone would be actionable under the Fourth Amendment as the plaintiffs could not point to a substantiated instance of government surveillance).

162. *See T.L.O.*, 469 U.S. at 329 (determining whether the search in question was unreasonable for the purpose of suppressing uncovered evidence in the subsequent delinquency charges).

163. *Id.* at 337.

164. Thanks to Marc Weber, Founder and Curator of the Internet History Program at the Computer History Museum, for bringing this salient point to the Author's attention.

165. Conor Dougherty, *Google Gives Child Pornography Evidence to Police*, The Bus. of Tech. Blog, N.Y. TIMES (Aug. 4, 2014, 9:41 PM), http://bits.blogs.nytimes.com/2014/08/04/google-gives-child-pornography-email-evidence-to-police/?_php=true&_type=blogs&_r=0.

any time, thus demonstrating the expansion of school authority under cyberbullying laws far beyond the boundaries of school and the school day.

### *C. School Surveillance Authority and the General Limits on Government Surveillance*

#### 1. Government Surveillance Authority Generally

Although doctrine on state surveillance authority has not addressed school surveillance authority, because the school is an arm of the state, this doctrine too is instructive. In 2012, the Supreme Court addressed state surveillance authority when it took up a challenge to § 1881a of the Foreign Intelligence Surveillance Act of 1978[166] in *Clapper v. Amnesty International USA*.[167] Section 1881a authorizes United States government surveillance of people who are not United States citizens and who are reasonably believed to be outside the United States.[168] The plaintiffs in *Clapper* were attorneys as well as labor, media, and human rights organizations.[169] They alleged that because they had reason to be in communication with people who could be under § 1881a surveillance, they too could be subject to surveillance by the government.[170] As a result, they had "'ceased engaging' in certain telephone and e-mail communications" and had "undertaken 'costly and burdensome measures' to protect the confidentiality of sensitive communications."[171] Challenging § 1881a on Fourth and First Amendment grounds, they alleged "an objectively reasonable likelihood that their communications will be acquired" and that the "risk of surveillance . . . is so substantial that they have been forced to take costly and burdensome measures to protect the confidentiality of their international communications."[172]

The Supreme Court rejected the plaintiffs' claims on Article III standing grounds. The Court found the plaintiffs' alleged injuries "highly speculative."[173] Specifically, the Court found that the plaintiffs' speculative fears were that

> (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so,

166. 50 U.S.C. § 1881a (Supp. V 2006).

167. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

168. 50 U.S.C. § 1881a.

169. *Clapper*, 133 S. Ct. at 1145.

170. *Id.*

171. *Id.* at 1145–46.

172. *Id.* at 1146.

173. *Id.* at 1148.

> the Government will choose to invoke its authority under §1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures [will] satisfy §1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of [plaintiffs'] contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.[174]

Taking issue with the conjectural nature of the plaintiffs' assertions of injury in *Clapper*, the Court identified factors that would have, if satisfied, arguably make the injuries real and present. Had the plaintiffs' contacts been government targets, and the government then conducted surveillance on them with the blessing of the FISA Court, the plaintiffs would have had greater success establishing their injury.[175] Had they also been able to show that the surveillance of their contacts was successful and occurred while the plaintiffs were parties to those communications, then the plaintiffs likely would have succeeded in showing an injury that satisfied Article III standing requirements.[176]

### 2. How the Cyberbullying Laws Exceed or Nearly Exceed Limits on Government Surveillance Authority

While not a school surveillance case, *Clapper* offers some possible insight regarding limits on state and, therefore, school surveillance authority more generally. The fact that school surveillance authority under the cyberbullying statutes, in at least some states, could meet the requirements for showing an injury under *Clapper* is suggestive of the breadth of schools' authority. In *Clapper*, the Court first took issue with the fact that the plaintiffs may not have been subjected to surveillance at all, making their claims of injury speculative.[177] Unlike the plaintiffs in *Clapper*, however, students are quite clearly the targets of surveillance in states where schools have unlimited or nearly unlimited authority to monitor their online and electronic activity. Moreover, the students are in fact being monitored through the use of comprehensive monitoring systems offered by companies like Geo Listening and CompuGuardian.

---

174. *Id.*

175. *See id.* (finding no injury due in part to the plaintiffs' inability to substantiate their argument that they themselves were the target of any actual government surveillance).

176. *See id.*

177. *Id.*

Similarly, unlike the plaintiffs in *Clapper*, students in those schools and school districts have an argument that the surveillance authority granted under the cyberbullying laws fails to satisfy existing safeguards under the Fourth Amendment for the reasons articulated in Part II.B.2 of this Article. As already discussed, whether students would succeed in this argument is still an open question; however, that the argument even exists demonstrates the breadth of school surveillance authority.

Finally, students in schools and school districts using the services and products of companies like Geo Listening and CompuGuardian could show that surveillance is effectively used to intercept their particular communication. The companies that provide services and products to allow schools to conduct surveillance boast of their effectiveness at intercepting students' online and electronic information, indicating their success at the interception of the communications.[178] In sum, the surveillance authority under cyberbullying statutes in these schools and school districts pushes the boundaries of even the federal government's limits on surveillance authority as it arguably comes close to creating an injury or injuries—especially to the extent that students change their behavior or incur costs to avoid monitoring.

Students attending schools and school districts that have yet to use all the authority provided under the cyberbullying laws to conduct comprehensive monitoring would be less able to meet the elements set forth in *Clapper*. But the schools need only decide to pay money to a company like Geo Listening or CompuGuardian, and students would likely be able to overcome the problems that stymied the plaintiffs in *Clapper*. Thus, even in those schools and school districts, the surveillance authority under the cyberbullying statutes nearly exceeds general limits on government surveillance.

Although no doctrinal limits exist for school surveillance authority under cyberbullying laws, First and Fourth Amendment student-speech and search doctrines as well as the doctrine on general government surveillance provides a general outline for when and where students are subject to school authority and the extent of that authority. By allowing schools in most states to conduct surveillance of students whenever and wherever they are, cyberbullying laws run roughshod over these kinds of doctrinal limits – failing to take them as any kind of guide regarding how far school surveillance authority can legitimately reach. These statutes create a world where everywhere is "in school" and therefore vastly expand the reach of school authority. If that were all the cyberbullying laws did, the expansion of school

178. Wallace, *supra* note 16 (quoting the President of Safe Outlook Corporation as proclaiming the amount of information his product can collect that can help schools discipline students for online behavior).

authority might be justified in the name of more effectively halting cyberbullying. Yet the statutes do not stop there. They also implicate affirmative privacy harms.

## III. PRIVACY HARMS, MORE ACUTE IN SCHOOL

While the clearest harm to students from the school surveillance authority may be the discipline that follows, students are also subject to privacy harms—simply through the act of surveillance alone.[179] Litigants challenging government surveillance absent prosecution or other obvious injury have not been particularly successful.[180] Courts have instead tended to find that "mere surveillance creates no harms."[181] In response, surveillance and privacy scholars have devoted energy to identifying the harms associated with broad public and private surveillance on its own. These scholars have made compelling cases. In doing so, they have drawn on the First and Fourth Amendments to articulate the particular kinds, or the nature, of privacy that surveillance invades. These kinds of privacy also are affected by school surveillance under the cyberbullying laws. Furthermore, these identified privacy harms are also more acute because the school is the state actor in question, and students are the subject of the surveillance authority.

### *A. The Kinds of Privacy Implicated*

Before discussing the privacy harms implicated by the unprecedented surveillance authority granted schools by way of the cyberbullying laws, a discussion of the nature of privacy associated with that surveillance authority is warranted. As the Supreme Court has stated, the nature of the privacy right implicated in any particular case is significant because the Constitution "does not protect all subjective expectations of privacy, but only those that society recognizes as 'legitimate.'"[182] Privacy and surveillance studies scholars have discussed two kinds of privacy that are relevant in the school surveillance context: intellectual privacy[183] and quantitative privacy.[184]

179. See the example cited at the end of Part I.B.3.

180. *E.g.*, Richards, *supra* note 19, at 1934; Citron & Gray, *supra* note 19, at 272; Solove, *supra* note 19, at 498.

181. Richards, *supra* note 19.

182. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 654 (1995).

183. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

184. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV 62 (2013).

### 1. Intellectual Privacy

Professor Neil Richards has articulated the concept of intellectual privacy.[185] In essence, the theory of intellectual privacy is about the ability to develop ideas on one's own.[186] While Richards conceives of intellectual privacy as "a series of nested protections," the core is about the ability to consider, weigh, and think through one's own beliefs and thoughts.[187] More specifically, Richards defines intellectual privacy as "the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others."[188]

Richards conceives of intellectual privacy as having four elements.[189] The first and "core" element of intellectual privacy "is the freedom of thought and belief."[190] It covers all the thoughts and beliefs an individual has.[191] Spatial privacy is the second element, and it "refers to the protection of places—physical, social, or otherwise—against intrusion or surveillance."[192] It is an integral component to intellectual privacy because people need these spaces free of interference in order to develop their thoughts and beliefs.[193] The third element of intellectual privacy is the freedom of intellectual exploration.[194] This right protects the ability to develop new ideas and all the processes involved in doing so.[195] Finally, the fourth element of intellectual privacy is confidential communications.[196] As Richards explains, "[c]onfidentiality protects the relationships in which information is shared, allowing candid discussion away from the prying ears of others."[197] It protects information from disclosure to or by third parties.[198]

185. *See* Richards, *supra* note 19; Richards, *supra* note 183.

186. Richards, *supra* note 183, at 389.

187. *Id.* at 408.

188. *Id.* at 389.

189. *Id.* at 392.

190. *Id.* at 408.

191. *Id.*

192. *Id.* at 412.

193. *Id.* at 413.

194. *Id.* at 416.

195. *Id.*

196. *Id.* at 421.

197. *Id.*

198. *Id.* at 422.

When schools have the authority to conduct surveillance of students, the intellectual privacy of students is squarely impacted. Each element of intellectual privacy is affected. Students' freedom of thought and belief is infringed because cyberbullying laws give schools access to almost any thoughts and beliefs students express electronically, regardless of whether they have anything to do with cyberbullying. If a student expresses a private thought about the quality of a school research assignment electronically, the school would potentially have access to those thoughts. If a student expresses frustration with her parents' imposition of a curfew online, the school would potentially have access to that information as well.

Schools also have access to the electronic spaces in which students express themselves under the cyberbullying laws, and thus they encroach on their students' spatial privacy. The companies that collect students' online data go to these spaces — sometimes public and sometimes private—to obtain the data. They even look to the spaces of the students' keystrokes when collecting students' electronic information.[199]

To the extent students use those spaces to develop ideas, the school can invade students' freedom of intellectual exploration. Consider the student who questions a teacher's interpretation of a particular piece of literature. If a student expresses that idea online, the school would have access to it. Surely not all students are using their time online to express high-minded thoughts, but even less academic expressions of thought fall under the category of intellectual exploration. Even social communication about cliques and romantic alliances falls into the category of intellectual exploration for a teenager who is learning to navigate an increasingly complex social system as she matures. Thus, for students in the majority of states, the cyberbullying laws allow their schools to intrude upon this intellectual exploration.

When any electronic or online communication is made — at least in twenty-five or arguably thirty-two states—the confidentiality of the communication is gone. If a student communicates electronically to a friend, makes a comment on a blog, or posts on social media, most schools would have the authority to access these communications. Thus, the students' abilities to communicate confidentially online is significantly reduced. While it is true that this reduction in confidentiality could be somewhat counteracted if students tightened privacy settings on social media sites and applications, this solution is only partial at best. Students would have to be conscientious enough to monitor their privacy settings often so when the privacy policies of

199. Wallace, *supra* note 16.

the companies offering the applications and social media change, the students could reassess the scope of their privacy settings.[200]

As a result of these invasions, students' intellectual privacy is curtailed as a whole when exercised electronically. Given that 95 percent of teens are online, the number of students potentially affected by this curtailment can reasonably be called significant.[201] Surveillance of their intellectual activities and the invasion of their intellectual privacy runs counter to even their relatively limited in-school First Amendment freedoms. Also, as will be discussed in Part III.B, the potential these invasions have for undermining the creativity of students' thoughts and intellectual pursuits runs contrary to the purpose of school.

### 2. Quantitative Privacy

Professors Danielle Keats Citron and David Gray have expounded the concept of quantitative privacy, which focuses on how, how much, and how frequently surveillance and data collection occur.[202] They argue that what is troubling about data collection is how broad and indiscriminate it is.[203] Such collection, they posit, "intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement or other government agents."[204] In the context of the Fourth Amendment, Citron and Gray contend that if quantitative privacy rights are implicated, the Fourth Amendment reasonableness standard must come to bear on the search.[205]

Cyberbullying laws impinge on quantitative privacy.[206] They allow for the broad, indiscriminate collection of data by the state because they allow for schools to collect virtually any online or electronic data of any student in the name of ferretting out cyberbullying.[207] Because the school is no less an arm of the state than law enforcement, school

200. Facebook, for example, is notorious for regularly changing its privacy policies without ample and obvious disclosure to users. *See, e.g.*, Brian Fung, *Your Facebook Privacy Settings Are About to Change. Again.* WASH. POST, Apr. 8, 2014, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/08/your-facebook-privacy-settings-are-about-to-change-again/.

201. Madden et al., *supra* note 72.

202. Gray & Citron, *supra* note 184.

203. *Id.* at 73–82.

204. *Id.* at 72.

205. *Id.*

206. *See supra* Part I.B.2, Part I.B.3.

207. *Id.*

surveillance authority is state surveillance authority in all the states with cyberbullying laws. In most states, the state, by way of the schools, has the authority to hire companies to conduct electronic dragnets. There is virtually no limit on the ways the schools in those states (or the companies they hire) can collect data or the amount of data they collect. As previously noted, none of the information may actually be related to cyberbullying or school. Even in the fourteen activity nexus states, the surveillance authority is still broad and indiscriminate because the laws allow schools to conduct surveillance of all student online activity without limit as long as students are in school or at school-related activities. In these states, schools can collect data on students by virtually any means and in any quantity as long as they do so while the students are in school or doing something like riding a school bus or waiting at a school bus stop.

This broad surveillance authority also infringes on students' quantitative privacy because schools have unfettered use of the data collected. [208] While the cyberbullying laws authorize or require schools to discipline students when they discover cyberbullying, they are silent as to what the schools can do with any other information they learn. The schools, therefore, have no guidance as to whether or how to use the other information gathered through their electronic surveillance of students. As a result, the schools could choose to ignore any such information, use it to benefit the students, or use it in ways that harm the students.

### *B. How the Fact of School Surveillance Authority Exacerbates Privacy Harms*

Perhaps the intrusion into students' intellectual and quantitative privacy could be argued acceptable in the name of derailing cyberbullying and particularly its potential for tragic outcomes.[209] An argument exists that schools need this broadly expanded authority. Otherwise, cyberbullying—hard to catch and potentially devastating in its effects—may continue to go unaddressed and unabated. What entity better than schools to address the cyberbullying among students? Students attend schools mandatorily,[210] and they are there

208. *See* N.J. v. T.L.O., 469 U.S. 325 (1985) (finding school officials acted reasonably when they searched a student's bag and found evidence that was subsequently used against the student in a delinquency hearing).

209. The Sheriff investigating Rebecca Ann Sedwick's death said she was "absolutely terrorized on social media." Other girls taunted her and urged her to kill herself. Alvarez, *supra* note 9, at A1, A3. At least four student suicides in California are tied to online bullying. Thomas & Murphy, *supra* note 2.

210. Every state has a mandatory school attendance law. *See* Institute of Education Sciences, *State Education Reforms*, NAT'L CTR. FOR EDUC. STATISTICS, at tbl.5.1, http://nces.ed.gov/programs/statereform/tab5_1.asp (last visited Sept. 29, 2014) (providing the age of required school

for six or more hours per day.[211] Moreover, cyberbullying does happen among students.[212] Accordingly, it makes more than a little sense that the schools should have some responsibility for stopping cyberbullying when it happens. However, the laws do more than broadly expand school authority to unprecedented degrees, resulting in general infringements on students' intellectual and quantitative privacy. They also impose specific privacy harms that are made more acute because of the school setting. Three privacy harms that have been identified by privacy and surveillance studies scholars in other contexts are not only relevant in the school context but are also intensified by it. In an effort to address a real problem, then, the cyberbullying laws create new ones.[213]

### 1. Civil Liberties Harms

Surveillance infringing on intellectual privacy, quantitative privacy, or both creates civil liberties harms in the form of squelching the development of ideas or causing self-censorship after those ideas have formed.[214] As Neil Richards persuasively argues, without the freedom to develop ideas, the ideas may not develop at all. When people fear being watched, they think and act differently.[215] Surveillance then can serve as a form of social thought control.[216] It can lead to the suppression or failure to formulate creative, new ideas.[217] What is more, even if surveillance does not suppress new ideas, it can cause individuals to self-censor extant ideas so they do

---

attendance under each state's compulsory school attendance laws as of 2013).

211. The average length of a public school day in the United States is 6.7 hours. Institute of Education Sciences, *Average Length of School Day in Hours for Public Elementary and Secondary Schools, by Level or School and State: 2007–08*, NAT'L CTR. FOR EDUC. STATISTICS, http://nces.ed.gov/surveys/AnnualReports/data/xls/daylength0708.xls (last visited June 25, 2014). In some states, students spend more than 1,000 hours of instructional time in school per year. Thomas D. Snyder & Sally A. Dillow, *Digest of Education Statistics 2011*, NAT'L CTR. ON EDUC. STATISTICS 253 (June 2012), http://nces.ed.gov/pubs2012/2012001.pdf.

212. To cite just two examples, the events prompting California to pass one of the first cyberbullying laws occurred between students as did the bullying events leading up to Rebecca Ann Sedwick's suicide in 2013. Alvarez, *supra* note 9; Thomas & Murphy, *supra* note 2.

213. Additionally, they do so without really addressing the causes and effects of bullying. *See infra* Part III.

214. Richards, *supra* note 19, at 1948–49.

215. *Id.* at 1948; Solove, *supra* note 19, at 494–95.

216. Solove, *supra* note 19, at 494.

217. Richards, *supra* note 19, at 1948.

not get expressed.[218] Surveillance makes people "extremely uncomfortable."[219] Simply put, innovative ideas or ideas that may be perceived as controversial are harder to express in an atmosphere of discomfort.[220]

It is for this reason, among others, that Richards calls for the protection of intellectual privacy. Richards argues that without its protection, individuals cannot develop the ideas and beliefs necessary to exercise their First Amendment rights.[221] Freedom of speech lacks meaning if individuals cannot engage in the processes necessary or have the space necessary to develop their own thoughts and ideas to then exercise their First Amendment rights.[222] Whether new or extant, if ideas cannot be developed or expressed, as Richards notes, the First Amendment protections lose substantial significance.[223] Freedom of speech and expression mean little when individuals cannot develop the ideas in the first place or fear sharing them with others.

When schools can conduct broad surveillance of students, students face these civil liberties harms. The only difference between students facing these harms and individuals in the public facing them more generally is that for students the harms are more acute because the school holds the authority. The harms are more acute because they stand in direct opposition to the purpose of school. Schools' function is to educate "the young for citizenship."[224] This means that schools serve to "[inculcate] 'fundamental values necessary to the maintenance of the democratic political system.'"[225] Indeed, educational philosopher and reformer John Dewey considered education to be an integral part of the right to vote.[226]

Yet when schools have the authority to conduct broad, comprehensive surveillance of students, students suffer civil liberties harms and fail to learn the values necessary for participation in democracy. Surveillance can have a chilling effect on their willingness to articulate ideas, particularly because students are increasingly using electronic means to communicate their ideas and thoughts as

218. *Id.* at 1949.

219. Solove, *supra* note 19, at 493.

220. *Id.*

221. Richards, *supra* note 183, at 389.

222. Richards, *supra* note 19, at 1946–47.

223. Richards, *supra* note 183, at 389.

224. Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 507 (1969).

225. Bethel Sch. Dist. No. 406 v. Fraser, 478 U.S. 675, 681 (1986) (quoting Ambach v. Norwick, 441 U.S. 68, 76–77 (1979)).

226. Erica Frankenberg & Chinh Q. Le, *The Post-Parents Involved Challenge: Confronting Extralegal Obstacles to Integration*, 69 OHIO ST. L.J. 1015, 1034 (2008).

compared with in-person or phone communication.[227] If their ability to develop new ideas is compromised, they cannot reasonably learn how to become engaged members of a democracy, where ideas are the bedrock of discourse and the informed vote.[228] School authority to conduct broad, comprehensive surveillance, then, suppresses rather than imbues the values of citizenship and democracy in students.

Of course, one purpose of any cyberbullying law and any attendant surveillance authority is to prevent students from engaging in cyberbullying by not only rooting it out but also preventing it quelling the speech before it happens. Yet, broad surveillance of students has the potential to do much more than quiet cyberbullying. It can stifle a much broader array of speech, teaching students to not participate in the intellectual exchanges that form the basis for democratic participation.

2. Imbalance in the State–Citizen Power Relationship

Another harm of surveillance is a change in the "power dynamic between the watcher and the watched" with the increase in power going to the watcher.[229] Neil Richards as well as Professor Daniel Solove both effectively contend that this change in the power dynamic between the state and citizens can result in harms such as discrimination and blackmail.[230] Surveillance is a tool of power.[231]

227. A 2012 Pew Research study found that 63 percent of teens communicate by text message daily while only 39 percent and 35 percent communicate over cell phones or in person, respectively. Amanda Lenhart, *Texting Dominates Teens' General Communication Choices*, PEW RESEARCH INTERNET PROJECT (Mar. 19, 2012), http://www.pewinternet.org/2012/03/19/communication-choices/. Although it can be argued that applications such as Snapchat, which create ephemeral messages that disappear after being read, reduce or eliminate any chilling effect, that argument fails to consider that even Snapchat messages can be saved by either the sender or the receiver. *Snapchat Guide for Parents*, *supra* note 43, at 6.

228. While it may be that much of students' online and electronic communications have much less to do with high-minded democratic debate and more to do with clothes, student romance, and the like, that does not mean that students do not engage in debates that are meaningful and foster their participation in the democracy. For example, in *Doninger v. Niehoff*, the student in question engaged in a debate online about a school official's decision to move the date or location of a student event. Though perhaps done in an inappropriate way, the debate about whether this could be done was ultimately one about school authority and student rights. Doninger v. Niehoff, 642 F.3d 334, 339–41 (2d Cir. 2011).

229. Richards, *supra* note 19, at 1953.

230. *Id.* at 1935; Solove, *supra* note 19, at 540–41.

231. Richards, *supra* note 19, at 1952–53; Solove, *supra* note 19, at 493.

When the power is increased such that the watcher has the tools to categorize people, the power can "bleed imperceptibly into the power of discrimination."[232] While not all discrimination is bad, surveillance allows the unfettered ability to classify people by type, which can lead to unwanted or unlawful discrimination.

This change in the power dynamic also can lead to blackmail.[233] The sheer amount of data that can potentially be collected through surveillance can lead to the revelation of individuals' secrets.[234] This information can easily be used against watched individuals for the gain of the watcher.[235]

In the school setting where the school is the watcher and the students are the watched, these harms are intensified for at least two reasons. First, schools already hold a larger proportion of power over students than does the state generally in the state–citizen relationship.[236] Schools have increased authority to infringe on students' First Amendment rights as well as their Fourth Amendment rights, and they have limited liability when they do cause students harm.[237] Coupling this already-extant power imbalance with the amount of information that schools can obtain on students via surveillance authority under the cyberbullying laws only intensifies the power imbalance.

Second, schools have a recurring history of engaging in discrimination, and students are particularly vulnerable to its harms. The ongoing series of school segregation cases attest that schools are not strangers to discrimination.[238] As burgeoning members of the adult social and economic spheres, students depend on schools to help them enter and navigate those worlds. Discrimination or blackmail can hamper or even destroy students' abilities to reach their potential in these arenas. This result could happen in myriad ways. Schools could discriminate against students based on surveillance in large or small forms, such as by determining who gets into honors classes based on surveillance data, thus potentially affecting students' college

232. Richards, *supra* note 19, at 1957.

233. *Id.* at 1953.

234. *Id.*

235. *Id.* (citing, by example, the use of information gained from FBI wiretaps of Dr. Martin Luther King Jr. to later blackmail him).

236. *Supra* Parts II.A, II.B.

237. *Id.*; *see also infra* note 238 and accompanying text.

238. The most famous of these cases involved racial segregation and occurred decades ago. Brown v. Bd. of Educ., 347 U.S. 483 (1954); Swann v. Charlotte-Mecklenburg Bd. of Educ., 402 U.S. 1 (1971); Milliken v. Bradley, 418 U.S. 717 (1974). However, desegregation cases continue today. *E.g.*, Everett v. Pitt Cnty. Bd. of Educ., 678 F.3d 281 (4th Cir. 2012).

admissions. Similarly, surveillance information could be used to blackmail students by incorporating it into a threat to withhold school services. Failure to receive school services, such as effective guidance services, could lead to problems getting jobs or into college after graduation. Of course, to be fair, the schools do have to control student behavior as reflected in any school discipline code. However, the maintenance of discipline in school is distinct from the use of vast amounts of data to control students' behavior, especially through means such as discrimination or blackmail.

### 3. Incorrect Data

Finally, surveillance can cause harms when the data collected are incorrect or incorrectly interpreted. Professors Citron and Gray point out examples of the problems that result from incorrect or incorrectly interpreted data.[239] These harms include employers' not hiring individuals based on erroneous data and the incorrect identification of individuals as potential terrorists or security threats.[240]

In school, the problem of incorrect or incorrectly interpreted data is as challenging or more so. As previously noted, the authority schools have over students' lives and futures is significant. It includes, on the low end of the spectrum, control over which activities, classes, and electives students participate in. These all may have an impact on students' futures since college admissions offices consider all of those factors in their decision making. This problem also spans to more direct control over students' ability to get into college or find work after high school because they need recommendations and assistance from school staff to be considered for admission or employment. To the extent that school staff are insufficiently helpful in these endeavors because of incorrect or incorrectly interpreted data gained from school surveillance of student online and electronic activity (as opposed to out of a desire to discriminate or blackmail students), the impact can be large and long lasting.

The harms derived from incorrect or incorrectly interpreted data as well as the civil liberties harms and harms from the increased imbalance in the state–citizen or school–student power dynamic are also exacerbated by the fact that students cannot avoid them. Students are required to attend school because every state has a mandatory attendance law.[241] Therefore, when a state has the authority to conduct broad surveillance of students, escaping the surveillance and its harms is nearly impossible.

In addition, when these harms occur, schools have almost no liability. As already noted earlier, no cyberbullying statute has a

239. Gray & Citron, *supra* note 184, at 80–81.

240. *Id.*

241. *See supra* note 210 and accompanying text.

cause of action. Indeed, fourteen states' cyberbullying laws expressly provide schools with immunity from liability under cyberbullying laws or deny any cause of action under them.[242] North Dakota's bullying legislation, for example, states that it does "not create or alter any civil cause of action."[243] Similarly, schools have very limited tort liability.[244] While schools have been held responsible for causing physical harm to students, these have only been in extreme cases.[245] The federal appellate courts have not held schools responsible for the imposition of severe emotional harm on students.[246] As a result, students who suffer privacy harms related to school surveillance have little to no recourse.

## IV. MOVING FORWARD: LIMITING SCHOOL SURVEILLANCE AUTHORITY AND PROTECTING STUDENTS FROM PRIVACY HARMS

The cyberbullying laws, for all the good intentions that underlie their passage, have not only vastly expanded school authority but have also created a new set of problems for students in the form of privacy harms.[247] Accordingly, while they are a well-meaning start to addressing the challenging, painful problem of cyberbullying, the laws need to be changed in two ways to limit school surveillance authority and any attendant privacy harms. This Part proposes these two

242. ALASKA STAT. § 14.33.230 (2012); ARK. CODE ANN. § 6-18-514(g) (2013); DEL. CODE ANN. tit. 14, § 4112D(e) (2011); FLA. STAT. § 1006.147(6) (West 2011); GA. CODE ANN. § 20-2-751.4(c) (2012); IOWA CODE § 280.28(5) (2011); MD. CODE ANN., EDUC. § 7-424(4) (2012); MASS. GEN. LAWS ch. 71, § 37O(i) (West 2013); NEV. REV. STAT. § 388.137 (LexisNexis 2013); N.H. REV. STAT. ANN. §§ 193-F:7, F:9 (2011); N.D. CENT. CODE § 15.1-19-2193 (2013); OHIO REV. CODE ANN. § 3313.667(c) (LexisNexis 2009); OR. REV. STAT. §§ 339.362(3), 339.364 (West 2011); TENN. CODE ANN. § 49-6-4505(c) (2013).

243. N.D. CENT. CODE § 15.1-19-22 (2013).

244. Immunity from tort liability still exists in a number of states. *See* Mark C. Weber, *Disability Harassment in the Public Schools*, 43 WM. & MARY L. REV. 1079, 1145 (2002).

245. *See id.*; *see generally* Emily F. Suski, *Dark Sarcasm in the Classroom: The Failure of the Courts to Recognize Students' Severe Emotional Harm as Unconstitutional*, 62 CLEV. ST. L. REV. 125 (2014) (analyzing why students' substantive due process claims have only succeeded in the federal courts of appeals in cases of extreme physical pain, such as when students have been hit by school officials, but not emotional harm, such as when school officials have caused post-traumatic stress disorder and suicidal ideation).

246. *See* Suski, *supra* note 245, at 128 ("No federal court of appeals, however, has found a student's severe emotional harm alone unconstitutional.").

247. *See supra* Part III.

changes. Specifically, it calls for a framework for limiting schools' surveillance authority and for the addition of a cause of action to the laws so students may seek recourse when schools exceed that authority. A framework for determining the boundaries of school surveillance authority is necessary because while schools do need some authority to monitor students' online activity beyond the school setting, they do not need as much authority as they currently have, particularly because of the imposed privacy harms.[248] They need the ability to intervene outside the physical school building in some instances because they are the natural arbiters of disputes between students when those problems impact school. When and how far beyond the school setting and into places like a student's bedroom that school authority should reach, though, is another matter. A meaningful framework can set the limits for this authority.

A cause of action in the cyberbullying laws is also necessary because students need a mechanism to enforce any such limits on schools' surveillance authority. As just discussed, the cyberbullying laws do not provide students with any means for recourse when the schools exceed what limits may exist on their surveillance authority and impose privacy harms. This change also will help limit school authority and the attendant privacy harms created by the cyberbullying laws by providing a means for controlling school authority and redressing privacy harms.

### *A. Limiting Schools' Surveillance Authority: The Nexus Standard Works and Why It Works*

Limiting the broad expansion of school authority under the cyberbullying statutes and the attendant privacy harms requires a framework for determining the outer limits of school authority beyond the physical school setting. Part II explains how cyberbullying laws expand school authority. That only takes the matter so far, though. It explains why the cyberbullying laws now are too broad but does not provide a framework for evaluating how far school surveillance authority should be allowed to go beyond the physical setting of the school.

The nexus framework articulated by the Fourth Circuit in *Kowalski v. Berkeley County Schools*, while developed in the context of a First Amendment analysis, provides a useful starting point for evaluating how far school surveillance authority should extend more

248. Schools already do a fair amount of surveillance on students while they are in school in ways other than by monitoring their online and electronic activity, such as "having law enforcement present on campus, controlling access to school grounds by locking or monitoring gates, and installing security cameras." Jason P. Nance, *School Surveillance and the Fourth Amendment*, 2014 WIS. L. REV. 79, 82 (2014).

generally.[249] In *Kowalksi*, the Court required a sufficient nexus between the school's pedagogical interests and the student's actions to justify the discipline.[250] This nexus standard provides a helpful framework for the evaluation of school surveillance authority for at least two reasons. First, it necessarily limits the school authority to instances in which the school has a substantial interest in and relationship to a student's actions as they occur. Second, some of the cyberbullying statutes already require a substantial nexus to school before triggering the school authority to monitor or discipline students' online or electronic activity.[251] They therefore offer at least a partial way forward for the rest—the bulk—of cyberbullying laws: providing an applicable framework that can serve the purpose of curbing cyberbullying while keeping school authority within reasonable limits and protecting students' from school-imposed privacy harms.

To accomplish this, the nexus requirement must be specifically and explicitly tied to the authority to conduct surveillance of students, as distinct from a school's ability to discipline a student for cyberbullying when it happens. More precisely, a school's ability to conduct surveillance should be tied to location and subject to the reasonableness requirement of the Fourth Amendment. While in *Kowalski* the Court declined to address the "metaphysical question" of where Internet conduct occurs, the question nonetheless must be addressed in order to adequately determine the breadth and limits of school surveillance authority.[252]

Indeed, the metaphysical question of where school boundaries start and end in the context of school surveillance authority is not that thorny when it is tied to location, and more specifically the location of students who either send or receive cyberbullying messages. Consider, for example, an alternative: using time as the metric for determining the boundaries of school surveillance authority. That nexus might link school authority to times when students are doing school-related activities. However, students could be engaged in school-related activity at any time. They could arguably be engaged in school-related activities at home while doing homework in their bedrooms. If school surveillance authority were so limited under the cyberbullying statutes, it would either amount to a complete limit or not much of a limit at all. Not knowing when students engage in school-related activities could leave schools in a position where they never monitor students' online activity unless students are in school

249. Kowalski v. Berkeley Cnty. Schs., 652 F.3d 565 (4th Cir. 2011).

250. *Id.* at 573.

251. *See supra* Part I.B.1.

252. Kowalski, 652 F.3d at 573.

because that is the only time they are surely engaged in school or school-related activities. Alternatively, it could also provide schools with the argument that they can conduct surveillance at almost any time since they have no way to know when students were engaged in online or electronic school-related activity. Thus, time offers an unworkable metric.

Location of the students provides a better, simpler limit on school surveillance authority. If surveillance power is tied to student location, then a meaningful limit is imposed on that authority. To flesh this nexus out further and more explicitly, the cyberbullying laws should only allow schools to conduct surveillance of students' online and electronic activity if students are at school or a school-sponsored activity. The latter should be defined broadly to include when students are on school vehicles, at school bus stops, or at school-sponsored events. The question that then arises is how schools would know whether students are at school or school-sponsored events. The old-fashioned methods of taking attendance would suffice for many, if not most, activities. However, it would not suffice for all. Football games, for example, are school-sponsored activities that typically do not involve attendance-taking. Yet even at these kinds of events, schools have at their disposal metal detectors, cameras, and other means of knowing which students are or are not at the events.[253] While one could very reasonably quibble with whether this level of essentially on-campus surveillance should occur, it does occur and courts have upheld schools' use of these methods.[254] Thus schools can use this technology to know whether students are at such school-sponsored events.

This location nexus works to allow schools to gather information in the name of determining whether cyberbullying might be occurring, but it still limits it. Location-nexus restriction still allows for broad data collection, but it does not allow it wherever and whenever the data might be generated or received. Schools have a much better argument for broad data collection when students are at school or school-sponsored activities because they have that interest in learning of any threat to the "order, safety, and well-being of students"[255] when they are in locations that render them essentially in school custody.[256] Location makes sense too in that the relationship between school surveillance authority and space defines what it means to be in school. Of course, the fact that this nexus is the nexus used by twelve

253. Nance, *supra* note 248, at 96.

254. *Id.*

255. *Kowalski*, 652 F.3d at 573.

256. Nance, *supra* note 248, at 133 (describing the responsibilities schools have for students' well-being and safety).

states serves to show that it does not so limit school authority to a place outside the mainstream.

Surveillance of students at school or at school-sponsored activities will still potentially be broad in that it can involve more than a few students; therefore, the surveillance needs to be subject to the Fourth Amendment reasonableness standard. As for the Fourth Amendment reasonableness standard, as articulated in Part II, the cyberbullying laws arguably breach this standard to begin with. Why, then, is this standard not sufficient? First, it requires students to know when they are being monitored. For many students, they may not know. The authority, though being used for comprehensive monitoring in some places, is still inchoate in many others. Thus, the search may or may not occur. The privacy harms occur because of the potential for the search, but the search itself need never occur for the harm to be rendered. Thus, the reasonableness standard alone does not fully protect students or limit school authority to conduct surveillance of them.

If a school, for example, has no cause to think cyberbullying may be happening in school or among students, then schools still should not be conducting surveillance of students. It would not meet the "justified at its inception" test required of student searches under *T.L.O.*[257] And even if a school does have cause to believe cyberbullying is happening, the school should still limit the scope of surveillance to as few students as possible in order to meet the scope requirement of *T.L.O.*[258]

Limiting schools' access to their online and electronic activity in these ways will protect students from privacy harms. These limits will provide students with space free of the watchful eye of the schools to express themselves online and electronically and thereby decrease civil liberties harms. Also, these limits will help to provide more balance in the power relationship between the state, in the form of schools, and the citizen-students by limiting state authority over students. Additionally, by limiting the information the schools have, these limits address concerns about incorrect or incorrectly interpreted data.

These limits on school surveillance authority also mean that that school may not catch some, even a lot, of cyberbullying through surveillance of students' online and electronic activity. To the extent that cyberbullying messages are being sent and received when students are not in school or at school-sponsored activities, schools could not catch it through surveillance. This is not to suggest, though, that cyberbullying occurring outside school or school-sponsored activities should not be caught or addressed. It does mean,

257. N.J. v. T.L.O., 469 US 325, 341 (1985); *see supra* Part II.B.

258. *T.L.O.*, 469 U.S. at 341.

however, that it would not be revealed by means of school surveillance.[259] Schools cannot be responsible for rooting out and addressing all cyberbullying whenever and wherever it happens. Parents and the rest of society have a responsibility to identify and address cyberbullying as well.

It should also be noted that this nexus framework is distinct from any nexus to the school authority to discipline students. The nexus is about school surveillance. The task of this Article is not to address whether schools can discipline students for behavior like that in *Kowalski*, should they learn of its existence.[260] The focus here is instead on limiting schools' authority to conduct comprehensive, indiscriminate surveillance of students' online and electronic activity anytime, anywhere.

### *B. Why Not an Ownership Nexus or the First Amendment Foreseeable Disruption Standard*

One might wonder why ownership is not a sufficient nexus or the First Amendment foreseeable disruption standard is not offered as the standard for determining the bounds of school surveillance authority. After all, ownership of equipment seems to come implicitly with the right of control. Moreover, the First Amendment foreseeable disruption standard has for decades provided a means for determining when schools could, usually by way of student discipline, regulate student speech.[261] The primary reason is that neither offers a meaningful limit on school surveillance authority.

Ownership is not a sufficient nexus because it still allows schools to monitor all students' online and electronic activity. With such a nexus, if students use schools' equipment, then the schools could monitor all students' online and electronic activity whenever and wherever it occurs.[262] In that case, the limit on school surveillance authority is not much of a restriction, especially for the lower-income student.[263] Rejecting an ownership nexus does not mean that schools cannot control their devices given to students. As noted above, they can and should be able to control their devices but do not need to

259. Certainly, truly horrifying behavior such as threats to seriously harm students and videos of sexual assaults may not be caught by school surveillance. That does not mean such activity cannot be discovered and addressed through other legal avenues, such as criminal search and prosecution.

260. *Kowalski*, 652 F.3d at 567 (noting how a student "creat[ed] and post[ed] to a MySpace.com webpage . . . which was largely dedicated to ridiculing a fellow student").

261. Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969).

262. *See supra* Part I.B.2.

263. *Id.*

comprehensively monitor students' online and electronic activity to do so.

Under the foreseeable disruption doctrine, if the speech would "materially [disrupt] classwork or involves substantial disorder or invasion of the rights of others," then it could be regulated by the school.[264] This standard provides little guidance for when schools can monitor student online and electronic activity. Any speech might materially disrupt the school no matter when or where it occurs. So using this standard would still arguably allow the schools to monitor students' online and electronic activity no matter when or where it occurs because it might materially disrupt the school.

### *C. A Cause of Action*

Because no cyberbullying statute has a cause of action, students have no clear recourse if schools exceed their authority under the cyberbullying statutes or impose privacy harms on them.[265] This failure to provide students with a cause of action serves to further exacerbate the already-extant power imbalance imposed by the cyberbullying statutes.[266] To better balance the power between student-citizens and the state in the form of schools, students need a cause of action so they can seek a remedy when they suffer privacy harms or schools exceed the authority granted under the cyberbullying laws. Cyberbullying laws, therefore, need to be revised to include both the location nexus proposed here and a cause of action for students should schools exceed it.

In order to ensure that students really do have a remedy under cyberbullying laws for excessive surveillance or privacy harms, the cause of action needs to more than simply exist in the statutes or apply to instances when the schools exceed the authority granted them in the statues. The provisions in the laws must also explicitly state that students can seek remedies for harms such as quelled speech, discrimination, blackmail, or other adverse effects they may have suffered from broad, indiscriminate surveillance, or incorrect or incorrectly interpreted data.[267] How a student might sue for quelled speech likely seems less obvious than how one would sue for blackmail and discrimination as there are already ways to seek redress for blackmail and discrimination in other areas of law. One quelled speech claim a student could make, by way of example, is that the student's

264. *Tinker*, 393 U.S. at 513.

265. *See supra* Part III.B.3.

266. *See supra* Part III.B.1–2.

267. To make the cause of action truly effective, of course, students will also need lawyers. While only the wealthier students could afford a lawyer to file a lawsuit, the benefits of such lawsuits would surely inure to the low-income students.

speech has become so limited due to the comprehensive surveillance by the school that the student has no electronic or online forums in which she can safely, without the watching eyes of the school, express her ideas. As a result, she can sue for both injunctive relief and damages for the loss of privacy and to ensure the school limits the surveillance so she does have electronic means of expressing herself without the school knowing about it.

This proposal for a cause of action in cyberbullying statutes could be criticized on a couple of fronts. First, critics could argue that the Fourth Amendment provides a remedy, obviating the need for an additional statutory cause of action. As explained in Part II, students do have an argument that schools violate the Fourth Amendment when they conduct surveillance of their online and electronic activity. This potential constitutional claim, however, does not suffice as a vehicle for limiting schools' surveillance authority and student privacy harms for at least three reasons. First, since the courts have not touched on whether this argument is valid, it is now just an argument. Second, that argument is not foolproof. A court would likely apply *Acton* as precedent for determining the reasonableness of broad school surveillance of student online and electronic activity instead of *T.L.O.*, since school surveillance is more like the suspicionless drug testing in *Acton* than it is the suspicion-based search in *T.L.O.* However, under the *Acton* standard, the school would have a decent argument that the surveillance is reasonable. While not as limited a search as the drug testing in *Acton*, the argument exists that school surveillance does respond to a strong need for school intervention and discipline in order to combat cyberbullying, much like the searches in *Acton*. Finally, the Fourth Amendment protects against intrusions when a legitimate expectation of privacy exists and has thus far tended to address injuries, like the use of unlawfully obtained evidence in prosecutions, or the denial of participation in a school activity.[268] It has not protected against "mere surveillance,"[269] suggesting there may be no legitimate expectation of privacy in students' online posts.[270]

Similarly, students also have limited recourse when making privacy claims in tort. School officials have substantial immunity against privacy and other tort claims.[271] Therefore, for all these

268. N.J. v. T.L.O., 469 US 325, 341 (1985) (student subjected to delinquency proceedings after marijuana-dealing supplies found in her purse); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) (discussing how student was "denied participation in his school's football program when he . . . refused to consent to [drug] testing").

269. Richards, *supra* note 19, at 1934; Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

270. *See supra* Part II.B.2.

271. Weber, *supra* note 244.

reasons, a cause of action under cyberbullying laws offers a clear way to provide students with needed means of recourse for overly broad surveillance and privacy harms.

A second criticism of the call for a statutory or regulatory cause of action is that because the cyberbullying laws will have to be amended to include these changes, the process will be slow or may not happen at all. Amending statutes and regulations is no small matter, politically or procedurally. However, the rapidity with which states have enacted these laws gives reason to think they could be amended just as quickly.[272] Admittedly, state legislators may be far less likely to rapidly enact ways to sue schools, but that does not make the solution in the form of the cause of action less necessary. When the stakes—students' privacy rights—are so high, the solutions that would offer real protection should be crafted regardless of the procedural difficulties.

It is worth stating here too that in addition to not providing any mechanism for redress for students, the cyberbullying statutes do little, or nothing in most cases, to address the root causes of cyberbullying: bullying more generally or its effects on victims. They are simply disciplinary statutes,[273] and most typically that discipline comes in the blunt forms of either suspension or expulsion.[274] Although this issue is beyond the scope of this Article, these failures in the cyberbullying laws are worth at least identifying alongside their other failures.

## V. CONCLUSION

Students need protection from cyberbullying, and schools are an obvious place to turn for providing at least some of that protection. Schools have students in their custody for six or more hours a day for the majority of the year, and cyberbullying often occurs among

272. Most cyberbullying statutes and regulations have been enacted since 2008. *See* Thomas & Murphy, *supra* note 2. Admittedly, states may not work as quickly to enact laws giving students a way to sue schools. However, the ability to quickly enact laws to protect students, which is what the quickly enacted cyberbullying laws represent, exists. Thus, the capacity exists to quickly amend those laws to include causes of action that would serve to better protect students.

273. For example, Indiana's bullying statute is part of its school disciplinary code. IND. CODE § 20-33-8-0.2 (2007). Utah's bullying statute calls for the suspension or expulsion of students for "behavior or threatened behavior which poses an immediate and significant threat to the welfare, safety, or morals of other students or school personnel or to the operation of the school." UTAH CODE ANN. § 53A-11-904(1)(c) (LexisNexis 2013).

274. IND. CODE § 20-33-8-0.2 (2007); UTAH CODE ANN. § 53A-11-904(1)(c) (LexisNexis 2013).

students.[275] In examining the cyberbullying laws across the states, this Article has identified the problematic ways these statutes have sought to provide that protection by calling attention to the unprecedented expansion of school authority embodied in those laws. The laws expand school authority in a majority of states so far beyond the traditional schoolhouse gates that anywhere and everywhere is arguably "in school." As well intentioned as the laws may be and as necessary as a response to cyberbullying is, the laws also implicate privacy harms for student that are made more acute because of schools' authority over students. The laws, therefore, need to be reworked. A nexus framework that is subject to Fourth Amendment reasonableness requirements linking school surveillance authority to when students are at school or school-related activities—needs to be imposed on the laws. Also, the laws need to provide students more agency in the form of a cause of action so they can seek redress when schools exceed their authority and impose privacy harms. Then the laws will better work to protect students, place meaningful limits on school authority, and prevent privacy harms on students.

275. *See supra* notes 6, 211, and accompanying text.